Sprehe Information Management Associates, Inc.
1301 Pennsylvania Ave., N.W.
Suite 507
Washington, DC 20004-1701
(202) 638-4333
Fax: (202) 638-2248
Internet: jtsprehe@access.digex.net

A STUDY OF POLICY ISSUES AFFECTING THE DEFENSE TECHNICAL INFORMATION CENTER

FINAL REPORT
(Revised)
Report for a Research Project

submitted to

The Defense Technical Information Center

by

J. Timothy Sprehe, Ph.D.
Sprehe Information Management Associates, Inc.

October 25, 1994

CONTENTS

EXECUTIVE SUMMARY ES-1

CHAPTER I. INTRODUCTION 1-1
- A. DTIC's Changing Policy Environment 1-1
- B. The General Situation of Scientific and Technical Information 1-3
- C. Study Approach 1-4
- D. Method of Study 1-5

CHAPTER II. THE CURRENT FEDERAL INFORMATION POLICY ENVIRONMENT 2-1
- A. The Privacy Act 2-2
  - 1. Privacy Protection Act 2-2
  - 2. Limits on Public Records 2-3
  - 3. Medical Records 2-3
  - 4. The IITF Draft Paper 2-5
  - 5. The OTA Report on Information Security and Privacy 2-6
  - 6. Forecast 2-8
- B. The Paperwork Reduction Act 2-9
  - 1. Current Efforts to Reauthorize the PRA 2-9
  - 2. Forecast 2-11
- C. Network-Related Legislative Proposals 2-11
- D. OMB Circular No. A-130 2-13
  - 1. Current Revisions to A-130 2-14
  - 2. The IITF Working Group on STI 2-16
  - 3. Forecast 2-16
- E. Federal Records Management 2-17
  - 1. PROFS Case and Electronic Records 2-17
  - 2. Government-wide E-Mail 2-18
- F. Federal Printing 2-18
- G. The GILS Movement 2-20
  - 1. Background 2-20
  - 2. The Draft OMB Bulletin 2-21
  - 3. Forecast 2.22
- H. The National Information Infrastructure 2-23
  - 1. Information Infrastructure Task Force 2-23
- I. The Solomons Conferences 2-24

CHAPTER III. FREEDOM OF INFORMATION ACT 3-1
- A. New FOIA Policy in Clinton Administration 3-1
- B. Electronic Freedom of Information Act Principles 3-2
- C. Electronic Freedom of Information Act 3-2

D. "Public Information" versus "Non-Public Information" 3-4
E. Forecast 3-6

CHAPTER IV. INTELLECTUAL PROPERTY 4-1
A. IITF Working Group Report 4-1
B. An Industry Framework for Managing Intellectual Property 4-3
C. Software Copyright 4-5
D. Open Source Intelligence and Copyright 4-6
E. Forecast 4-9

CHAPTER V. INDUSTRY VIEWPOINT ON FEDERAL INFORMATION DISSEMINATION 5-1
A. Introduction 5-1
B. The Information Industry Association 5-2

CHAPTER VI. STI AND FEDERAL INFORMATION POLICY 6-1
A. Government Information "versus" Scientific and Technical Information 6-1
B. Statistical Policy Directives 6-2
C. Other Ways of Classifying Government Information 6-3
D. How STI Is "Different" 6-5
E. A Policy Circular for STI? 6-7
1. Policies Directly Applicable 6-7
2. Policies Indirectly Applicable 6-8
3. Policy Areas Omitted from OMB Circular A-130 but Important to STI 6-8
4. Bringing in Established Policies 6-9
F. Who Would Issue the Policy? 6-10
G. STI Policy and the National Science and Technology Council 6-11

CHAPTER VII. CONCLUSION 7-1
A. Summary of Forecasts 7-1
B. Concluding Recommendations for DTIC 7-3

APPENDIX A. LIST OF PERSONS INTERVIEWED

A STUDY OF POLICY ISSUES AFFECTING THE DEFENSE TECHNICAL INFORMATION CENTER FINAL REPORT

EXECUTIVE SUMMARY

I. INTRODUCTION

This is a report of a research project sponsored by the Defense Technical Information Center (DTIC) for the purpose of exploring the federal information policy environment in which DTIC finds itself today. DTIC serves as a central depository and secondary distribution center for the collection, storage, and dissemination of scientific and technical information (STI) resulting from or pertinent to the Department of Defense (DoD) research and development efforts. Documents reach DTIC when their "controlling agents" send them to DTIC, providing four designations pertaining to the release of the documents.

The policy environment in which the Defense Technical Information Center (DTIC) lives is changing rapidly today. In the post-Cold War era, Congress and the administration have begun to exert increased pressures on federal research and development and to insist on setting of priorities within the R&D budget. The administration of the Freedom of Information Act (FOIA) could be changing. The Clinton administration initiatives in the National Information Infrastructure (NII) impact on DTIC. Among other things, the NII is placing renewed emphasis on making government information quickly and easily available to the general public through instrumentalities such as the Internet.

DTIC is an information center that deals principally in federal scientific and technical information (STI), a subset of the universe of federal information that has its own issues and problems. Issues affecting STI are its definition; technology transfer; interagency coordination; standards; infrastructure; international questions; and access to and dissemination of government information. Sprehe Information Management Associates (SIMA) has undertaken this six-month study of the DTIC policy environment. The study was intended to describe and characterize DTIC's current operational framework and policy framework from the viewpoint of an outsider with a broad information policy background; identify coming institutional and policy changes that will impact on DTIC; and recommend how DTIC should position itself to anticipate and take advantage of these changes. The report summarizes findings and makes recommendations as to how DTIC should position itself to take best advantage of coming changes.

SIMA studied -- and this report describes -- DTIC's current situation, through observation, interviewing and reading. The author characterized coming changes affecting DTIC by reviewing literature and interviewing key actors both within and outside DTIC.

II. THE CURRENT FEDERAL INFORMATION POLICY ENVIRONMENT

The second chapter of the report presents a selective overview of recent developments in federal information policy. Federal information policy is a set of laws and policies, sometimes not well integrated with one another, that spell out how the federal government will behave with respect to information and information technology. The primary emphasis here is on information management, as distinguished from information technology management.

A. The Privacy Act. S. 1735, the Privacy Protection Act was a bill calling for establishment of a Privacy Protection Commission, an independent advisory agency with five commissioners, which would ensure that privacy rights are protected, particularly with respect to electronic data. The chief difficulty, from the administration's viewpoint, appeared to be the problem of proliferating too many federal agencies and where to place a new entity within current governmental organization, how to balance independence and relevance in the organizational placement of a new entity for privacy advocacy. The bill did not pass in the 103rd Congress but might very likely pass in the future in a different form.

Legislative efforts have recently been made to limit access to public records such as those in state departments of motor vehicles. A bill sponsored by Senator Boxer would have prevented disclosure of names and addresses of vehicle owners except for routine uses such as public safety, civil criminal proceedings, research activities, and insurance. Major opponents of the bill are firms in the direct marketing business, who see any curtailment of access to public records as impacting on their livelihood. Some limitations on access may be enacted into law, but in view of the strong commercial interests supporting access and the solid public policy reasons for maintaining access, they will be watered down.

Today, no uniform federal law or policy governs an individual's records as a patient in the health care system, and state laws are a crazy quilt of privacy coverage. Most people never dream of the myriad uses made of their health care information when they visit a doctor today. What the country will need as part of health care reform is a uniform code of fair information practices to govern health care information. Proposals for such a code are based on eight principles: openness; individual participation; collection units; data quality; limits on use; disclosure limits; security; and accountability. Representative Gary Condit (D-CA) introduced into the 103rd

Congress' debate over health care reform a bill concerning fair health information practices which was intended to be attached to whatever health care reform legislation was passed. Individually identifiable information created in the health treatment or payment system would become "protected health information." Almost everyone who has access to or handles protected health information would become a "health information trustee." The debate over health care has also drawn considerable attention to potential uses of smart cards and to whether individuals should be given national identifier numbers; both issues present major privacy problems.

The Information Infrastructure Task Force's Working Group on Privacy issued a draft report entitled "Principles for Providing and Using Personal Information" in May 1994. The report attempted to articulate an information privacy principle, information integrity principles, and sets of principles for information collectors, for information users, and for individuals who provide personal information. At this writing the Working Group is redrafting its report.

In September 1994, the Office of Technology Assessment published *Information Security and Privacy in Network Environments*. Noting the expanding use of information networks in business and government and the fact that major concerns for the security and privacy of information in network environments are at present unresolved, OTA examined cryptography policy, guidance on safeguarding unclassified information in federal agencies, and legal issues with respect to information security. The report discussed the diminishing government monopoly on cryptographic expertise and the debate over the Clipper chip. Intense public debate over Clipper caused Congress to ask the National Research Council for a major study of the issues.

Privacy and security issues are "hot" topics in federal information policy, so that one can expect Congress in 1995 to revisit the questions of a privacy commission, restrictions on access to public records, security and privacy on networks, and fair health information practices.

B. The Paperwork Reduction Act. The name "Paperwork Reduction Act" (PRA) was applied to a law whose scope is much broader than limiting the amount of information the government collects from its citizens; the Act gives six functions to OMB, only one of which is paperwork control. The Act also created the Office of Information and Regulatory Affairs in OMB which has been the locus for administering presidential initiatives for deregulation. The question of reauthorizing the PRA has been enmeshed in regulatory and small business politics. In the 103rd Congress, the Senate eventually passed a compromise bill, S. 560 which extended into every aspect of the original legislation. The bill maintained the primary focus on eliminating unnecessary paperwork burdens and added several additional purposes such as improving the delivery of services to the public. The bill quite explicitly aimed to overturn *Dole v. United Steelworkers of America*, the Supreme Court's decision regarding

third-party information disclosure requirements. It set forth agency responsibilities in greater detail, and shifted emphasis away from OMB, conceiving OMB as providing policy and oversight but not as second-guessing agency decisions. The bill added the new function of information dissemination to the six previously in the Act; new provisions gave specific guidance on information dissemination. Prospects are fairly good that the bill might pass the Senate again in the next Congress. Whether the House and the Senate will agree on a version of the PRA in the 104th Congress is anyone's guess.

C. Network-Related Legislative Proposals. Much of the action in federal information policy during the 103rd Congress occurred in legislation related to the information superhighway. Important bills were introduced by Senator Hollings (S. 4), Rep. Boucher (H.R. 1757), Senator Kerrey (S. 626), and gathered together in H.R. 820. None passed the Congress but they are sure to arise in the future.

D. OMB Circular No. A-130. The philosophy that informed the original 1985 version of OMB Circular No. A-130 grew out of the atmosphere of the early years of the Reagan White House. OMB published its first official revision to Circular A-130 in July 1993, and followed that with a second revision in July 1994. The circular has now abandoned the strong emphasis on the private sector. In addition to redressing some obvious deficiencies of the original circular, especially the role of records management and coordination with state and local governments, the circular now devotes much of the information management section to information dissemination. The circular now directs that the senior official for information resources management in each agency act as an ombudsman to "consider alleged instances of agency failure to comply with this Circular and recommend or take corrective action as appropriate." The circular's Section 8b, Information Systems and Information Technology Management, now leads off with a set of statements about evaluation and performance measurement. OMB especially stresses benefit-cost analysis of information systems. Greatly minimized in the new A-130 is the doctrine of chargeback for information processing services, the notion that programmatic users of federal computer centers must pay for all computer services.

Coupled with the 1993 rewrite of information management policy, the new version almost finishes the task of completely rethinking the original A-130 issued in 1985. The chief piece not yet recast is the circular's appendix on computer security, an increasingly thorny political issue because of the White House's commitment and industry's opposition to the Clipper chip. In general, the 1993-1994 revisions to A-130 are good news for agencies such as DTIC.

E. Federal Records Management. If everything transpiring on an agency's electronic mail system is legally a federal record, then everything on the system must be preserved. And everything will sooner or later be open to public scrutiny. These

contingencies are real possibilities depending on the final aftermath to *Armstrong v. Executive Office of the President*, the case in which the National Security Archives sued the White House to prevent the destruction of the "PROF" tapes from the Iran-Contra scandal. What the judge's opinion in the case means for federal agencies is that they must be able to prove they have established a well defined relationship between e-mail and federal records, and they must be able to show that agency records officers are supervising how staff decide which e-mail messages are records and which are not. While the case is still dragging on, NARA issued a notice of proposed rulemaking on electronic mail systems in March 1994. At the same time, the White House wants to develop an electronic mail system within the federal government. The idea is to interconnect government e-mail to public services to improve citizen participation in government.

F. Federal Printing. Under legislation passed in 1993, the Government Printing Office now offers the *Congressional Record* and the *Federal Register* as online services. The principal effect of this legislation was to provide GPO with a license to produce and disseminate electronic information products. As part of the National Performance Review, the Clinton administration announced that it wants to institute federal printing reform. The administration's legislative proposal was politically unrealistic, expecting Congress to remove an executive branch problem whose removal would cause Congress itself the problem of what to do with GPO's 5,000 employees. The administration's legislative proposal for federal printing did not pass the Congress. In September 1994, OMB Director Rivlin announced that the administration would maintain the *status quo* in federal printing through 1995 while still seeking to accomplish a comprehensive legislative reform of printing.

G. The GILS Movement. The movement toward a federal information locator system has been alive for at least twenty-five years. The basic concept is that the federal government should have some unified vehicle that the general public could use to locate information among the vast number of publications issued. The Paperwork Reduction Act of 1980 (PRA) included language establishing the Federal Information Locator System (FILS). As a finding aid for locating government publications, FILS was essentially useless. The statutory FILS concept focused on information *inputs* to government, whereas the interests of those needing a finding aid were in the information *outputs* from government. An additional difficult was the fact that the PRA charged OMB with responsibility for maintaining and operating FILS and OMB never adequately discharged the responsibility.

On September 22, 1994, OMB circulated for comment the draft of an OMB Bulletin intended to establish the Government Information Locator Service. Agencies are required to establish publicly available inventories of their print and electronic publications in a common format to be promulgated in a Federal Information Processing Standard that the National Institute of Standards and Technology will issue.

The FIPS will define a "GILS core," a bare minimum of data elements that each agency must adhere to. Every agency must create a locator database that holds at least the GILS core.

What will be achieved when a government-wide information locator is in place? The important thing is not to do the locator once, but to put it into place in such a way that it continues year after year. Since DTIC already publishes *How to Get It*, GILS could be an opportunity for DTIC to offer to make this publication the basis of a DoD-wide GILS. GILS also represents a threat to DTIC in terms of moving DTIC toward providing services direct to the public. DTIC may well be concerned, as are other agencies, that advertising the existence of records systems will result in a significant increase in FOIA requests which, in turn, could prove sufficiently annoying to DoD components as to cause diminution in the flow of documents to DTIC -- an undesirable outcome. Hence DTIC must carefully evaluate the costs and benefits of GILS.

H. The National Information Infrastructure. The National Information Infrastructure encompasses an integrated web of telecommunications, information, and computing technologies. The vision of the NII is to interconnect businesses, governments, researchers, educators, and the public with advanced communication and information resources throughout the nation. The administration established the Information Infrastructure Task Force (IITF) to coordinate policy and implementation. Among the NII bodies created in 1994 was a working group on STI established under the Government Information Working Group of the IITF.

I. The Solomons Conferences. Beginning in 1991, officials in the offices of information resources management in major federal agencies held interagency conferences on public access to electronic government information. The conferences were initially held at Solomons, Maryland, and became known as the Solomons conferences. The proceedings of these conferences show that the agencies are developing their own public access policies, somewhat independent of OMB; that the policies are remaining at a very general level; and that the agencies do not have budgeted resources to devote to public information dissemination programs. While the early Solomons conferences restricted participation to federal agency personnel, more recent conferences have opened the doors to public interest groups as well.

III. FREEDOM OF INFORMATION ACT

The Freedom of Information Act (FOIA) is intended to be a basic guarantor of openness in government. FOIA provides that the records of government shall be available for access to the public, upon request, at a nominal charge, subject to nine exemptions.

A. New FOIA Policy in Clinton Administration. The Clinton administration

announced a new policy on administering FOIA. The Justice Department will no longer defend an agency's withholding of information merely because there is a 'substantial legal basis' for doing so. Rather, in determining whether or not to defend a nondisclosure decision, Justice will apply a presumption of disclosure. It does not appear that the new ground rules will substantially alter the way agencies conduct their FOIA business; so far it seems like business as usual. In this sense, there may be little real significance, other than as a symbol, to the Clinton administration's new posture on FOIA.

B. Electronic Freedom of Information Act Principles. In mid-1994, an interagency group completed a draft document entitled something like "Principles of Electronic FOIA." Reportedly, it contained 66 principles that the agencies believed should government electronic FOIA. The author was unable to secure a copy in time for inclusion in this report.

C. Electronic Freedom of Information Act. Electronic FOIA is usually understood to mean that, if an agency possesses the requested information in electronic format, and if the requester asks for the information in electronic format, and assuming the request does not fall under the Act's exemptions, the agency must provide the information in electronic format. In the 103rd Congress, Senator Leahy introduced S. 1782, the Electronic Freedom of Information Improvement Act of 1994, a bill to require agencies to publish indices of their electronic information holdings, to make all regulations available electronically, and to make reasonable efforts to provide information in formats requested by the public.

One fear that electronic FOIA has engendered in federal agencies, particularly OMB, is that, were the law clarified, commercial database vendors might be given a license to go shopping through agency databases in search of commercially exploitable databases. These critics argue that the FOIA was intended to promote openness in democratic government rather than to serve as the basis for commercialization of government information. They believe that, before an electronic FOIA bill is passed, the nation needs a thorough debate on the Act's foundations and a means of balancing openness in government against commercial interests. In the event, the electronic FOIA legislation did not pass the 103rd Congress. Electronic FOIA is a topic that is very likely to arise and to be the subject of successful legislation in the 104th Congress.

D. "Public Information" versus "Non-Public Information." The term "public information" has now come into usage, meaning any information the agency makes public whether pursuant to law or policy. Many gradations can be devised between what is clearly not public information and what clearly is public information. The author suggests a classification of information into: non-public information; gray area non-public; and public information. Over time, the category of public information is growing and the gray area is shrinking. The advent of GILS will cause more pressure

on agencies to increase public information, even though the agencies do not have the budgetary resources to do so.

IV. INTELLECTUAL PROPERTY

A key issue in the new network environment in which federal agencies increasingly find themselves is the complex of issues surrounding intellectual property.

A. IITF Working Group Report. In July 1994, the intellectual property working group issued a preliminary draft of its report, titled "Intellectual Property and the National Information Infrastructure." The report treats first with law, examining the basic legislation for copyright, patent, trademarks, and trade secrets. The main focus of the legal treatment is copyright law. The working group recommends amending the Copyright Act in several respects for the network environment.

The report moves on to technology, looking at technology for controlling access to protected works, for controlling use of the work, for authenticating the work, and for managing rights in the work. The report notes that technology can defeat any protection technology itself provides. The working group realized that the problems faced in a national information infrastructure would be repeated and doubtless magnified in a global information infrastructure and recommended three principles on which rules would be formulated. This section ends with the development of technology standards. The report then treats briefly of education, and moves finally to its preliminary findings and recommendations which center primarily on legal issues.

B. An Industry Framework for Managing Intellectual Property. In March 1994, the Information Industry Association published a monograph titled *Protecting Intellectual Property Rights on the Information Superhighways*. The author suggests that eleven elements are necessary in developing a framework for the management of intellectual property. Another way to approach the question of managing intellectual property is to survey briefly the management practices in use by vendors in the private sector. The author examines the practices of vendors of online information services, of commercial CD-ROM publishers, and of software licensing in network environments. In the electronic environment, methods are being developed for protecting intellectual property, notably the concepts of software envelope and header.

C. Software Copyright. One of the areas in which the policy interests of STI agencies may diverge from those of other information programs and agencies is copyright protection for computer software. In recent Congresses, several efforts have been made to legislate a limited government copyright for federally generated software to enhance technology transfer. OMB's Office of Information and Regulatory Affairs, the home base for OMB Circular No. A-130, has generally taken the view that any

government copyright is an undesirable change in the Copyright Act. The STI agencies, on the other hand, are among those who argue that Congress should enact legislation providing limited copyright for federally developed software.

D. Open Source Intelligence and Copyright. As the intelligence agencies investigate information sharing across agency boundaries, they have discovered problems of incompatible systems that inhibit sharing. One solution to these problems, particularly as regards open source intelligence, is to use a single common agency as a repository and central distribution point for the information. Hence the agencies have turned increasingly to DTIC as a kind of clearinghouse.

For open source intelligence, agencies are beginning to make information available to the general public, as in the case of the CIA's Foreign Broadcast Information Service. So long as the agencies redact their sources and share within the federal government, no copyright problems arise. To the extent, however, that the agencies redisseminate whole works to the general public from their open source holdings, they will encounter problems of copyright, especially as regards the Berne Convention. Under the Berne Convention, agencies must assume that open source intelligence is copyrighted. In handling open source intelligence for other agencies, DTIC will seek out copyright holders and pay the commercial prices for products.

V. INDUSTRY VIEWPOINT ON FEDERAL INFORMATION DISSEMINATION

In addition to statements from the Computer Systems Policy Project, the Council on Competitiveness, the Information Technology Association of America, the Coalition for Networked Information, and the Electronic Frontier Foundation, the Information Industry Association has issued a white paper on federal information dissemination policy. The principles, based on three assumptions, assert that the government has a responsibility to assure broad access to public information. They advocate having agencies target information dissemination toward unmet needs in versatile formats. IIA particularly emphasizes the principle of diversity, the idea that the government should encourage the greatest feasible diversity of sources for public information. They want policies implemented through a meaningful, open, and workable compliance and review mechanism.

VI. STI AND FEDERAL INFORMATION POLICY

A. Government Information "versus" Scientific and Technical Information. In discussions of circular A-130, the question arose: what is the relationship between "government information," on the one hand, and [government] "scientific and technical information" (STI) or [government] "statistical information," on the other? The answer is that government information is the most general term; STI and statistical information are subsets of government information. Hence, A-130's policies apply to STI, but STI

policies might not apply to all government information.

B. Statistical Policy Directives. This distinction between government information as the whole and government STI/statistical information as the part has been recognized in practice for many years. OMB's Statistical Policy office issues "Statistical Policy Directives" which have the force of OMB circulars. At present there are 19 such directives, some of which are dynamic and even controversial.

C. Other Ways of Classifying Government Information. Among the many ways of classifying government information, Molholm has suggested grouping government information into the following classes: consumer information, citizen information, administrative (or operating) information, business information, and STI. In his analysis, the gradations of government information are distinguished by whether or not they require further processing in order to be understandable and useful to the general public.

D. How STI Is "Different." The question to ask about STI is this: are there important areas of information law and policy that pertain specifically to STI and are inadequately treated in general information policy? The answer is yes.

The polarized organizational and cultural setting of STI is different from other kinds of government information. At one pole is the *culture of science and academia*, because much of the government's STI is generated by scientists in the nation's colleges, universities, and research institutes. Scientific and academic culture maintains an imperative in favor of the widest possible dissemination of information. At the other pole is the *culture of classified information and export controls*. These cultures are characterized by an imperative favoring containment of information; the fewer people who have access to information, the better. STI is also *international* in scope, not regarding national boundaries. One consequence of the international nature of STI is that STI policy is to a considerable extent intermixed with and affected by *foreign policy*.

E. A Policy Circular for STI? The environment in which STI lives has distinctive policy issues that do not pertain to all government information.

1. Policies Directly Applicable. Policies directly applicable to STI include *federal research and development policy* and *technology transfer policy*.

2. Policies Indirectly Applicable. Policies indirectly applicable to STI include *information classified for purposes of national security* and *export control information*.

3. Policy Areas Omitted from OMB Circular A-130 but Important to

STI. Circular A-130 omits in-depth treatment of *international issues* and *interagency sharing* of information. STI agencies are heavily involved in both of these arenas and could profit from central policy guidance.

4. Bringing in Established Policies. Arguably, a number of existing policy areas and documents could be incorporated into an STI policy. Among these are *OMB Circular No. A-16;* policy on *treatment of human subjects in research;* and *Statistical Policy Directives Nos. 16 and 17.*

F. Who Would Issue the Policy? As to who should issue an STI policy, reasons can be given for having either OMB or OSTP -- or perhaps both -- promulgate government-wide STI policy.

G. STI Policy and the National Science and Technology Council. Now that the president has established the National Science and Technology Council, perhaps NSTC could be interested in developing and issuing government-wide STI policy.

VII. CONCLUSION

The report concludes by summarizing the forecasts made in the foregoing chapters. Finally, the author offers a set of recommendations for DTIC concerning GILS, intellectual property, FOIA, and government-wide STI policy.

A STUDY OF POLICY ISSUES AFFECTING THE DEFENSE TECHNICAL INFORMATION CENTER

FINAL REPORT
(Revised)

CHAPTER I

INTRODUCTION

This is a report of a research project sponsored by the Defense Technical Information Center (DTIC) for the purpose of exploring the federal information policy environment in which DTIC finds itself today.

A. DTIC's Changing Policy Environment

DTIC serves as a central depository and secondary distribution center for the collection, storage, and dissemination of scientific and technical information (STI) resulting from or pertinent to the Department of Defense (DoD) research and development efforts. Authorized users can access DTIC's information holdings through the Defense Research, Development, Test and Evaluation Online System (DROLS) which consists of three major databases.

1. **The Technical Report Database** contains citation to two million documents in a broad range of subjects. Documents classified for purposes of national security make up ten percent of the database; 40 percent are limited in distribution; the remainder are unclassified and unlimited in distribution.

2. **The Work Unit Information System (WUIS) Database** is a collection of technically oriented summaries describing proposed and ongoing DoD research and technology efforts.

3. **The Independent Research and Development Database** contains descriptions of proposed and ongoing technical effforts funded solely by private sector funds of potential interest to DoD and other federal R&D agencies. This database is proprietary and only available to DoD components and other federal agencies approved for access by DoD.

DTIC does not retail its services direct to the public. Those unclassified,

unlimited distribution technical reports that DTIC makes available to the public are actually distributed by the Commerce Department's National Technical Information Service under an interagency agreement.

Documents reach DTIC when their "controlling agents" send them to DTIC. The process of sending a document to DTIC involves completion of Standard Form 298 and providing four designations for the document.

1. Whether the document is **classified** for purposes of national security;

2. Whether the document is **proprietary**;

3. Whether the document is **export controlled**;

4. A **distribution statement** indicating how the document is to be distributed and why it has been given this designation.

The policy environment in which the Defense Technical Information Center (DTIC) lives is changing rapidly today. Several current developments suffice to illustrate these changes. First, in the post-Cold War era, Congress and the administration have begun to exert increased pressures on federal research and development and to insist on setting of priorities within the R&D budget.[1] Legislation has been enacted to identify priorities for dual-use technologies to serve both national security and economic prosperity goals. Priority setting has also recently occurred for cross-cutting interagency programs. The process of setting budget priorities affects DTIC directly as well as indirectly through the actions of its supplying agencies.

Second, administration of the Freedom of Information Act (FOIA) could be changing. The Clinton administration has changed the presumption about how FOIA will be handled. Now, unless records are precluded from disclosure under the FOIA, the presumption is they should be disclosed. Further, the administration has signalled its openness to revision of the Act in the direction of "electronic FOIA." DTIC processes many FOIA requests annually. The effect of the new changes in policy is that DTIC must reexamine its policies and practices with respect to FOIA. This scrutiny may eventually cause DTIC to ask its supplying agencies in the Department of Defense to alter the manner in which they assign distribution statements to documents sent to DTIC.

---

[1]See Genevieve J. Knezo, "R&D: Priority Setting and Consolidation in Science Budgeting," CRS Issue Brief IB94009, Congressional Research Service, Library of Congress, August 29, 1994.

As a third example, the Clinton administration initiatives in the National Information Infrastructure (NII) impact on DTIC. Among other things, the NII is placing renewed emphasis on making government information quickly and easily available to the general public through instrumentalities such as the Internet. The administration's NII initiative also has created a Working Group on Intellectual Property as part of the Information Infrastructure Task Force (IITF). The working group has now published a paper on treatment of intellectual property in the NII. Treatment of intellectual property is an important issue for DTIC in its dealings with the intelligence community. Also, DTIC is a participant in a newly created IITF subgroup known as the A-130 Implementation Group which will examine how STI agencies are implementing the policies of OMB Circular No. A-130.

This study has examined changing conditions in the federal information policy environment as a prelude to understanding how changes might affect DTIC.

B. The General Situation of Scientific and Technical Information

DTIC is an information center that deals principally in federal scientific and technical information (STI). STI, as a subset of the universe of federal information, is a field that has its own issues and problems. The following paragraphs summarize some of these issues.

Definition. Scientific and technical information (STI) tends to get defined operationally. STI is what scientists and engineers do, the fruits of their basic and applied research. While this definition serves its purposes, this research project has moved beyond the question of definition. A more important question, from the author's point of view, is whether STI faces policies issues that are not well considered in current information policy, especially in OMB Circular No. A-130 and in various proposals to reauthorize the Paperwork Reduction Act? Does the statutory basis for STI provide ways to distinguish STI and the setting of STI agencies from other government information activities?

Technology Transfer. Much more so than other government information, STI exists within a framework that requires technology transfer. How does information figure as an integral component in technology transfer? How does technology transfer policy link up with federal information policy?

Interagency Coordination. STI is the responsibility of half a dozen or so agencies, and appears to suffer from a lack of definitive leadership. While the agencies are well coordinated under CENDI, no clear central direction for STI emanates from the Executive Office of the President. NTIS is now the beneficiary of STI under the American Technology Preeminence Act but it is not yet clear exactly how this will work out for the STI community. Moreover, far more than other kinds of government

information, STI tends to be multi-disciplinary and hence to require sharing of information among federal agencies.

Standards The rapid growth in the use of electronic information sources has led to a need for renewed attention to information standards in the STI field. The interdisciplinary nature of STI makes standards development of paramount importance because standards must satisfy the needs of many scientific disciplines.

Infrastructure. National attention is currently being drawn to the question of information infrastructure. The interdisciplinary nature of major policy concerns such as global climate change demands interdisciplinary communications patterns for interagency problem solving.

International. The conduct of science is increasingly international in scope. American scientists now must communicate regularly with scientists in other countries. The result of this is that STI is also reaching a far broader audience, sometimes global in nature. Federal agencies involved in STI find that their activities are enmeshed in foreign policy considerations.

Access and Dissemination. The phenomenon of electronic networking is sweeping the nation, not only in terms of local and wide area networks but also in the conglomeration of networks known as the Internet. The Internet arose to a large extent from the federal defense community and its needs for high speed remote access to information resources. Today's information access and dissemination environment makes it technically possible for persons operating computers from remote sites to log in and behave as local users, interacting electronically with other users and exchanging data files. To date, policy formulation in the federal information field has not kept pace with the technological potential.

Through its program and policy activities DTIC both affects the ways in which the above issues are resolved and is affected by the larger policy environment these issues imply.

C. Study Approach

The foregoing examples serve to demonstrate that DTIC would be well served to take a fresh look at the information policy environment in which it operates with a view toward anticipating change and being prepared to cope with it when it arrives.

Sprehe Information Management Associates (SIMA) has undertaken a six-month

study of the DTIC policy environment.[2] The study was intended to accomplish three things:

- Describe and characterize DTIC's current operational framework and policy framework from the viewpoint of an outsider with a broad information policy background;
- Identify coming institutional and policy changes that will impact on DTIC; and
- Recommend how DTIC should position itself to anticipate and take advantage of these changes.

To some extent, the study replicated, in much shortened form, Dr. Sprehe's experience in the drafting of OMB Circular No. A-130, except that this study concentrated exclusively on STI. One outcome of the study, therefore, was to explore whether there should be some semblance of A-130 for STI.

D. Method of Study

The study proceeded, first, by meeting and agreeing with DTIC concerning the number and scope of issues to be concentrated on, and selecting which officials inside and outside of DTIC should be interviewed.

Second, SIMA studied and this report describes DTIC's current situation through observation, interviewing and reading.

Third, the report characterizes coming changes affecting DTIC by reviewing literature and interviewing key actors both within and outside DTIC. The study gathered and analyzed the relevant descriptive and analytical documents concerning DTIC policy issues. Because of their scope and complexity, many of these issues have generated a substantial, publicly available literature of reports, studies, and even legislation.

Fourth, the report summarizes findings and makes recommendations as to how DTIC should position itself to take best advantage of coming changes. The report deals with STI policy issues in their general government-wide context and insofar as they touch upon DTIC specifically.

---

[2]The actual working time for the project was six months, beginning in February 1994 and ending on October 25, 1994. No work was performed during June and July 1994, in accordance with an understanding between SIMA and DTIC.

CHAPTER II

THE CURRENT FEDERAL INFORMATION POLICY ENVIRONMENT

The Clinton administration has introduced a period of great ferment and movement in federal information policy. Just the first year alone of the administration witnessed the enunciation of a presidential information technology policy,[1] the beginning of a quest for a national information infrastructure,[2] a major federal initiative in computer security policy in the so-called "Clipper chip,"[3] a milestone management appraisal of the federal government,[4] proposals to restructure fundamentally the institutional arrangements for federal printing,[5] and a new executive order on deregulation of the federal government.[6] This new "front-and-center" attitude toward information policy questions occurred despite the preoccupation with major legislative programs such as the crime bill and health care reform.

This chapter presents a selective overview of recent developments in federal information policy. Omitted from the chapter are treatments of the Freedom of Information Act and intellectual property. These two topics are treated separately in following chapters. Also omitted is consideration of efforts in 1994 to amend the Communications Act, which were unsuccessful, and the Leahy-Edwards Digital Telephony bill, which did pass the 103rd Congress in its last days. The chapter also does not deal with procurement reform legislation passed during the 103rd Congress.

Federal information policy is a set of laws and policies, sometimes not well integrated with one another, that spell out how the federal government will behave with respect to information and information technology. The primary emphasis here is on information management, as distinguished from information technology

---

[1]The White House, Technology for America's Growth: A New Direction to Build Economic Strength, February 22, 1993.

[2]The White House, *The National Information Infrastructure: Agenda for Action*, September 1993.

[3]See, for example, Digital Privacy and Security Working Group, "Privacy, Security and the National Information Infrastructure: An Overview," with six issue papers, available from the Electronic Frontier Foundation, Washington, DC, October 1993.

[4]Vice President Al Gore, *Report of the National Performance Review*, Washington, DC: Government Printing Office, September 1993).

[5]See, Title XXIV, H.R. 3400, 103rd Congress, the legislation proposed to implement the National Performance Review.

[6]The White House, *Regulatory Planning and Review*, Executive Order 12866, September 30, 1993.

management. That is, the study and this chapter concentrate less on how federal agencies manage their computers and telecommunications, and more on how they behave with respect to the information content of their work.

The principal laws embodying federal information policy are the First Amendment to the Constitution, the Copyright Act (Title 17, U.S. Code, especially Section 105), the Freedom of Information Act (Title 5, U.S. Code, Section 552), the Patent and Trademark Act, the Privacy Act (Title 5, U.S. Code, Section 552a), and Title 44. Title 44 contains the federal printing laws and the provisions concerning distribution and sale of public documents (Chapters 1 through 19); federal records and archives management (Chapter 21 through 33), and coordination of federal information policy (the Paperwork Reduction Act, Chapter 35). Many other laws bear on specific aspects of federal information policy, most notably the Brooks Act (the Federal Property and Administrative Services Act, Title 40 U.S. Code, Sections 759 and 487) which pertains to the acquisition and management of federal information technology (computers and telecommunications) and the Stevenson-Wydler Act which sets the parameters for technology transfer.

During the 103rd Congress, major legislative proposals were introduced that would make changes in federal information policy. These proposals are discussed below. Almost none of the proposals passed into law.

A. The Privacy Act

1. Privacy Protection Act. Concern has been growing in Congress and the public that application of today's information technology, while generally beneficial to society, holds the potential for massive invasion of privacy. As one indicator of this concern, the European Community has issued a draft directive on privacy that provides for differences in treatment with respect to exchange of personal data for countries that do and do not have data or privacy protection laws. Adoption of the directive could cause significant impact on U.S. agencies and firms doing business in Europe.

In November 1993, Senator Simon introduced S. 1735, the Privacy Protection Act. The bill called for establishment of a Privacy Protection Commission, an independent advisory agency with five commissioners, which would ensure that privacy rights are protected, particularly with respect to electronic data. The commission would provide the public with a central agency for guidance on privacy protection and fair information practices, and oversee federal agencies' compliance with the Privacy Act. It would also promote adoption of fair information practices. Also important is the fact that almost all developed nations have privacy commissions and the U.S. is at a disadvantage in international affairs for not having a privacy commission that can

represent U.S. interests.

Prospects were considered initially good for passage of the Simon bill. The Clinton administration's National Performance Review called for a commission to perform similar functions. The chief difficulty, from the administration's viewpoint, appeared to be the problem of proliferating too many federal agencies and where to place a new entity within current governmental organization. It would be important for the new agency to be perceived as having an independent voice, a factor that argues for creating an independent agency. At the same time, too much independence can lead to isolation and irrelevance; a tiny independent agency, far from the centers of power, would have little authority; as an example, consider the National Commission on Library and Information Services. The dilemma, then, is how to balance independence and relevance in the organizational placement of a new entity for privacy advocacy.[7]

2. **Limits on Public Records**. In California, actress Rebecca Schaeffer was brutally murdered in the doorway of her Los Angeles apartment by a man who had obtained her home address from the California Department of Motor Vehicles (DMV). The outcry over this and similar cases caused Senator Boxer to introduce the Driver's Privacy Protection Act in November 1993. In 34 states, anyone can go to the DMV with a license plate number and come out with the name and home address of the vehicle owner. The Boxer bill would prevent such disclosure except for routine uses such as public safety, civil criminal proceedings, research activities, and insurance. It would also limit uses for marketing purposes and for verifying personal information in business transactions. Major opponents of the bill are firms in the direct marketing business, who see any curtailment of access to public records as impacting on their livelihood.

3. **Medical Records**. Today, no uniform federal law or policy governs an individual's records as a patient, and state laws are a crazy quilt of privacy coverage. Computers are neither friend nor foe in this arena; they make some things easier and others far more difficult.

---

[7]The Presidential Reorganization Project in the Carter administration gave considerable attention to the question of how to reorganize the federal statistical system. The most argued point was where to place statistical policy in order to assure a strong central coordinating body. Some argued that a central statistical office should be created as an independent agency, pointing out that the statistical policy function was relatively powerless within the Office of Management and Budget. The prevailing argument, however, was that statistical policy should be beefed up but kept in OMB because proximity to the budget process was the primary insurance of the function's relevance. The Carter administration reorganized OMB and moved statistical policy to the Department of Commerce. The Congress placed the function back in OMB when it passed the Paperwork Reduction Act of 1980.

Most people never dream of all the uses made of their health care information when they visit a doctor today. Beyond the physician's present and future use of those notes for direct care, that information may go to nurses or laboratories to provide the person with additional care. It will be used to document the services rendered in order to collect payment, and be sent on to an insurance company for possible reimbursement. The insurance company itself will make multiple uses of the information, including actuarial analyses. Other uses of the information include aggregation into epidemiological studies of the spread of disease. Parts of the information will reach pharmacists who sell the person medicines. It will also find its way into the stores of data used in clinical studies and health care management analyses.

What the country will need as part of health care reform is a uniform code of fair information practices to govern health care information. The Department of Health and Human Services articulated one back in 1974. Several states have passed laws governing use of health care information, notably Washington, Massachusetts, and Montana. The HHS code, which could be the basis for a uniform federal statute, rests on eight basic principles:

1. Openness: No secret records.
2. Individual Participation: The ability to see and amend records.
3. Collection Limits: Limits on what information is collected.
4. Data Quality: Assurances of data accuracy and reliability.
5. Limits on Use: Use only for stated purposes.
6. Disclosure Limits: Limits on who can see and use the information.
7. Security: Assurances of data security.
8. Accountability: Those who keep the records must be accountable.

Two key issues affecting health information privacy are information technology and a national identifier. With respect to technology, many parties today are studying smart cards, credit card-sized devices containing integrated circuit chips which can act as a microprocessor. The idea is that an individual could carry around his or her detailed medical history on a smart card -- up to 800 printed pages, and produce the card for electronic information transfer with any computer encountered in the health care system.

To many the smart card looks like a good solution for the massive paperwork costs of health care, and several nations are experimenting with this approach. To others, the prospect of millions of citizens walking around with their most intimate secrets in their pockets or purses only multiplies and magnifies privacy problems. The chances for the information to fall into the wrong hands increase astronomically with the patient-borne smart card. For protecting privacy and confidentiality, one would have to rely on the intelligent behavior of each person carrying the smart card, and this

is not an inviting picture to privacy experts.

The second issue is the question of a national identifier. Proponents of the computerized patient record recommend the use of a unique patient identifier, a cradle-to-grave number. If that one number followed individuals around throughout life, the theory goes, so could all the health care information the individuals are bound to give rise to. These discussions lead naturally to the old idea that the U.S. should adopt the Social Security number as a national identifier. The SSN already links the individual to large bodies of information in federal databanks. More fundamentally, debate over a national identifier numbering system, an issue seen recently in debate over immigration reform, raises the specter of a Big Brother government capable of infiltrating the tiniest recesses of people's lives.

Representative Gary Condit (D-CA) introduced into the 103rd Congress' debate over health care reform a bill entitled the Administrative Simplification and Fair Health Information Practices Act. The bill was intended to be attached to whatever health care reform legislation had the greatest likelihood of passage. The bill was voted out of committee and seemed to have sufficient support to be included in a successful health care reform initiative, but no such initiative passed the 103rd Congress.[8] Like other analyses of the current situation in medical records, the Condit bill referred to the "patchwork" of current medical privacy laws and regulations, arguing a compelling need for federal intervention. Its purpose was to establish a code of fair information practices for health information. The bill used two basic concepts. First, individually identifiable information created in the health treatment or payment system is "protected health information." Second, almost everyone who has access to or handles protected health information becomes a "health information trustee."

In effect, the Condit bill chose not to define the privacy rights of the individual with respect to health information, concluding that a host of valid public policy reasons exists for intruding into the individual's medical privacy. Instead, the bill attached to the medical information itself a code of fair information practices. These practices would follow the information into all the many places it goes and pertain to whomever gains access to the information. The practices themselves are consistent with the fair information practices enumerated above.

4. The IITF Draft Paper

The Information Infrastructure Task Force's Working Group on Privacy issued a draft report entitled "Principles for Providing and Using Personal Information" in May

---

[8]See Committee on Government Operations, *Health Security Act*, House Report No. 103-601, August 12, 1994.

1994 and asked for public comment.[9] The report attempted to articulate an information privacy principle, information integrity principles, and sets of principles for information collectors, for information users, and for individuals who provide personal information. The principles were accompanied by an explanatory commentary.

The initial work of the IITF Privacy Working Group was deemed unsatisfactory by much of the community that follows privacy matters. The principles the group set forth seemed empty and the commentary sententious. The draft contained principles for individuals, collectors, and users, but not for information carriers. The U.S. has a large body of law and regulation governing information carriers, the communications industry, but the principles overlooked this fact.

The commentary that came with the IITF's principles indulged in philosophizing. For example, an individual's subjective expectations of privacy were to be honored only if "objectively reasonable," a term that is left unsatisfactorily defined. What if one person's "objectively reasonable" disagrees with another's subjective expectations?

Elsewhere the commentary said that it is impossible to formulate any set of principles that can cover comprehensively all possible uses of information, and that general principles cannot resolve difficult issues. Either these were meaningless statements or the commentary unwittingly argued against the very principles it was supposed to be explaining.

5. The OTA Report on Information Security and Privacy

In September 1994, the Office of Technology Assessment published *Information Security and Privacy in Network Environments.*[10] The report noted the expanding use of information networks in business and government and the fact that major concerns for the security and privacy of information in network environments are at present unresolved. OTA examined cryptography policy, guidance on safeguarding unclassified information in federal agencies, and legal issues with respect to information security.

The federal government still possesses the most expertise in cryptography, although the nongovernment market has grown rapidly in the last 20 years. Federal

---

[9]Privacy Working Group, Information Infrastructure Task Force, "Principles for Providing and Using Personal Information," draft for public comment, May 1994.

[10]Office of Technology Assessment, *Information Security and Privacy in Network Environments,* Washington, U.S. Government Printing Office, September 1994

export controls and the Federal Information Processing Standards (FIPS) developed by NIST have major impact on information safeguards based on cryptography. The government confronts a fundamental tension between fostering widespread use of cost effective information safeguards and controlling the proliferation of safeguard technologies that could impair U.S. intelligence and law enforcement capability. The government has tried to control cryptography through FIPS and export controls. Now export control arguments are joined with arguments concerning control of domestic crime in an effort to preserve government capabilities. Because communications technologies are now used widely by the general public as well as businesses, interest in information safeguards has also grown and manifests itself in the debate over key-escrow encryption, popularly known as the "Clipper chip" controversy.

The Clinton administration publicly embraced the Clipper chip in 1993. This escrowed-encryption initiative has met intense public criticism, stemming largely from privacy concerns and the fact that cryptographic keys will be held by federal agencies. Critics disparage the implementation of escrowed encryption through hardware rather than software, the possibility of mandatory usage in the future, and the general secrecy surrounding the administration's actions. In 1994, Congress asked the National Research Council to conduct a major review of cryptography and some urge a halt to the escrowed-encryption initiative until the study is completed in 1996. One outcome of this debate is development of more open processes for determining how cryptography will be deployed in American society. OTA suggested Congress should periodically examine how export controls as well as cryptography initiatives are deployed in the U.S. and lists some immediate initiatives Congress could pursue.

OTA also suggested Congress take a direct role in establishing guidance for how federal agencies safeguard information. OMB is shortly to release a revised version of the security appendix to Circular A-130. The OTA report suggested Congress ensure that agencies include specific provisions for safeguarding information in information technology planning, that agencies budget sufficient resources for information safeguard, and that NIST assign sufficient resources to implementing the Computer Security Act. OTA believed NIST has been overly deferential to the National Security Agency under the Act, ceding too much authority to NSA.

Under legal issues, the OTA report considers electronic commerce, noting that current law offers little guidance concerning safeguard techniques, a situation that has given rise to a diversity of security and authentication practices in electronic commerce. OTA points out the disparity in the level of personal protection for privacy in data in the U.S. as compared with European countries and the fact that the disparity may make it difficult to exchange data with these countries. Here OTA suggests establishing a federal privacy commission as a counterpart to the governmental bodies established in other countries. Finally, the report examines protection of intellectual property in the administration of digital libraries and finds the application of current law problematic.

The development of multimedia authoring tools raises new questions pertaining to copyright and royalties. Congress could take legislative action to further define the copyright law -- the alternative apparently preferred by the IITF report, let the courts continue defining electronic copyright law, encourage private rights-clearing and royalty-collection agencies, or allow development of private sector monitoring capabilities to support a fee-for-use basis for electronic copyrighted works.

5. Forecast

The Privacy Protection Act for establishment of a privacy commission did not pass in the 103rd Congress and in all probability will not pass in the future *in its current form*. The administration may agree to an amendment to the bill that would establish a presidential advisor on privacy, a member of the White House staff, while giving the staffing functions to one of the agencies, following the model of the consumer affairs arrangement.

While the mood of public opinion favors legislation such as the Boxer bill to limit access to public records, it bears remembering that these records are presently available to the public as a matter of law and that strong public welfare arguments underpin the laws. Making automobile, real estate, and other property records public has been one major way in which government has prevented fraud and swindles and has enforced public accountability. Some limitations on access may be enacted into law, but in view of the strong commercial interests supporting access and the solid public policy reasons for maintaining access, they will be watered down

With respect to medical privacy, the fair health information practices bill introduced by Rep. Condit in the 103rd Congress garnered enough support to become relatively nonpartisan and noncontroversial. Passage of such a bill is expected as an integral part of any health care reform the Congress enacts.

As of October 1994, the Privacy Working Group of the Information Infrastructure Task Force was in the process of revising its draft paper on the basis of public comments received. A new version of the paper should be issued by early 1995. The OTA report is a much more in-depth study of privacy and security issues, and it has the virtue of setting forth options in very clear terms. The OTA report is likely to be quite influential in molding congressional opinion concerning the issues.

DTIC does not have individually identifiable information in its holdings, so that actions in the privacy arena will not directly affect DTIC. However, developments in the security field are of direct interest to DTIC, and privacy and security are tightly intermixed. Privacy-security is one of the "hot" policy areas in which much can be expected to happen over the next several years.

B. The Paperwork Reduction Act.

The name "Paperwork Reduction Act" (PRA) was applied to a law whose scope is much broader than limiting the amount of information the government collects from its citizens. The Act is codified in Title 44 as Coordination of Federal Information Policy, and it charges the Director of the Office of Management and Budget with carrying out six functions:

1. General information policy
2. Paperwork reduction
3. Administration of the Privacy Act
4. Statistical policy
5. Records management and archival policy
6. Policy regarding information technology (automatic data processing and telecommunications).

The PRA also created the Office of Information and Regulatory Affairs (OIRA) within OMB, the unit responsible for administering the Act. Since its inception OIRA has also been the locus for administering presidential initiatives for deregulating the economy, and hence OIRA has encountered the problem of being associated more with deregulation than with information policy.

This problem has affected the PRA for several years and still faces the Act today. In 1989-1990, Congress tried and failed to reauthorize the PRA. The House passed a bill but the Senate failed to pass companion legislation. The public interest groups wanted a PRA that enunciates an aggressive position on disseminating government information, especially on opening up the storehouses of federal electronic databases for public consumption. They also wanted to open up to greater public scrutiny OIRA's regulatory review processes. They were less interested in federal paperwork burdens. The interests of these groups were generally carried forward in the Senate by Senator John Glenn, Chairman of the Senate Governmental Affairs Committee.

The small business community, on the other hand, wanted the PRA to continue doing what its title says: reducing government paperwork. Because OMB's regulatory review authority is often used to block onerous federal paperwork, they favored keeping OMB as a powerful hindrance to runaway agency regulations. And this community was much less interested in federal information dissemination policy. The small business community found its champion in Senator Sam Nunn, Chairman of the Senate Small Business Subcommittee on Government Contracting and Paperwork Reduction.

1. Current Efforts to Reauthorize the PRA

The conflicting interests of these two communities managed to stalemate reauthorization of the PRA in the 101st Congress, and the Bush administration did little to break the stalemate. Senator Nunn and Senator Glenn each introduced bills during the 103rd Congress to reauthorize the PRA. Eventually, the two senators agreed on a compromise bill which was reported out of committee in the Senate as S. 560 in August 1994. The compromise bill was a large one and extended into every aspect of the original legislation.

The Senate bill maintained the primary focus on eliminating unnecessary paperwork burdens and added several additional purposes such as improving the delivery of services to the public. The bill defined introduced several new definitions, two of which may be repeated here:

> The term *"information resources management"* means the process of managing information resources to accomplish agency missions and to improve agency performance, including through the reduction of information collection burdens on the public.
>
> The term *"public information"* means any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public.

The bill quite explicitly aimed to overturn *Dole v. United Steelworkers of America*, the Supreme Court's decision regarding third-party information disclosure requirements.[11] It set forth agency responsibilities in greater detail, and shifted emphasis away from OMB, conceiving OMB as providing policy and oversight but not as second-guessing agency decisions. The bill added the new function of information dissemination to the six previously in the Act; new provisions gave specific guidance on information dissemination. Statistical policy and records management functions were strengthened and spelled out in more detail. The bill placed more emphasis on information resources management, redefining the concept and taking other steps such as making OMB's five-year information technology plan into a five-year information resources management plan. It also revised agency responsibilities under the Act, clearly providing that responsibility for agency IRM rests squarely with the agency and that each agency is expected to take this responsibility very seriously. Agencies

---

[11] *Dole v. United Steelworkers of America*, 494 U.S. 266 (1990). The question at issue was whether a federal agency, using its authority under the PRA, can require third parties (e.g., product manufacturers) to disclose health and safety information via product labelling. The intent of S. 560 is to clarify that agency third-party information disclosure requirements are within the scope of the Act.

were to establish a senior management IRM steering committee. The bill reworked and expanded the language of the former Federal Information Locator System to bring it into harmony with current thinking about the Government Information Locator Service [see below].

Agency responsibilities for reducing paperwork burden on the public were substantially revised in the bill. There was now mandated a detailed information collection evaluation procedure, independent of program responsibility, to evaluate proposed agency information collections. The public comment period was reduced to a maximum of 60 days and agencies would have had to certify that each information collection met a new set of criteria.

The bill devoted considerable attention to agency information dissemination responsibilities. The new provisions were intended to guide agency dissemination activities and promote greater public access to government information in as many forms or media as possible. Agencies would have had to ensure that the public has timely and equitable access to government information, encourage a diversity of public and private sources, and generally act in an efficient, effective, and economical manner. The bill said agencies must disseminate information on a nondiscriminatory and nonexclusive basis. The bill prohibited four practices: exclusive or restricted distribution arrangements; restrictions on use or reuse of government information; fees or royalties for reuse or resale; and establishment of user fees that exceed the cost of dissemination.

2. Forecast

The PRA reauthorization did not pass in the 103rd Congress. The bill passed the Senate in the waning hours of the 103rd Congress, despite threats that various Senators would block the bill's overturn of the Dole case. Prospects are fairly good that the bill might pass the Senate again in the next Congress. The House passed its own version of a reauthorization in the 101st Congress, but whether the two bodies will agree on a version in the 104th Congress is anybody's guess. To some extent the impetus to reauthorize the PRA has lost steam in recent years. With the many competing interests chipping away at various pieces of the law, no effective coalition that might drive through a reauthorization has materialized. The administration can claim that it is already administratively implementing many of the desired reforms such as openness in regulatory review and a pro-dissemination information policy. Within the administration's crowded political agenda, the PRA appears to have secondary priority.

C. Network-Related Legislative Proposals.

Much of the programmatic impetus for federal information dissemination is now coming from network related legislation, as much as from the developments surrounding the Paperwork Reduction Act. S. 4, the National Competitiveness Act of 1993, introduced by Senator Hollings, contained, among other things, Title VI, the Information Technology Applications Act of 1994. This would have been the follow-on to the High Performance Computing and Communications Act (HPCCA), and would have established an information infrastructure program and development plan. The bill called for building digital libraries of electronic information accessible over the Internet, and proposed applications for education, manufacturing, health care, and libraries. The applications sections contained language supportive of general database access and use. S. 4 passed the Senate as an amendment to H.R. 820 in March 1993.

In the House, Rep. Boucher introduced H.R. 1757, the National Information Infrastructure Act of 1993. The bill built on HPCCA by adding a new title on Applications of Computing and Networking. The bill's Findings contained the following: "a coordinated interagency undertaking is needed to identify and promote applications of computing and networking advances . . . which will provide large economic and social benefits to the Nation, including new tools for teaching, the creation of digital libraries of electronic information, the development of standards and protocols to make the stores of government information readily accessible by electronic means, and computer systems to improve the delivery of health care." H.R. 1757 passed the House in July 1993 and was incorporated into H.R. 820.

The Boucher bill included applications for education (including K-12 access to databases), health care (including access to medical literature), libraries (including digital libraries technology), and government information. Each of the applications sections contained language on access and use of databases. The section on government information, for instance, was aimed at developments and applications for "improved public access to information generated by Federal, State, and local governments." Provisions included connecting depository libraries and other sources to the Internet to enable access to government databases, access to State/local government information, linkages with and access to related resources, and testing and evaluating new access and use technologies. The section also provided for a federal information locator.

Sen. Kerrey introduced S. 626 to establish a system of state-based electronic libraries. The bill would have established a grants program for state electronic libraries administered by NSF. It provided for access to federal databases and bibliographic information such as the Library of Congress. S. 626 was folded into S.4 which then became part of H.R. 820.

The Senate version of H.R. 820 did not pass, so the various pieces of network related legislation were one more victim of the failed agenda in the 103rd Congress. The key questions concerning network-related bills are whether and how these pieces of programmatic legislation are integrated with basic information policy legislation. How, for example, would these bills have protected principles of copyright when private firms add value and resell government information? How do the Internet proposals deal with user charges? How do they preclude monopolistic practices? How do they ensure timely and equitable access to all members of the public and a diversity of public and private sources? The answer is that they are probably not well integrated, that the legislation's drafters are generally unaware of federal information policy. For the moment, these questions do not matter, however, because the 103rd Congress adjourned without passing any of these measures into law. They are sure to arise again in the 104th Congress.

D. OMB Circular No. A-130.

OMB Circular A-130, the Management of Federal Information Resources, was issued as official policy in December 1985. The philosophy that informed the original document grew out of the atmosphere of the early years of the Reagan White House. Those were the days when the Defense Department was censoring the contents of scientific papers intended for presentation before scientific societies, and the trend toward declassifying documents was sharply reversed, resulting in substantial increase in numbers of classified documents. Those were the days when agencies were instructed to contract out their library services. Those were the days of the infamous government-wide moratorium on new publications. They were the days of the equally infamous newsphoto of Presidential Counsellor Ed Meese and OMB Deputy Director Joe Wright dumping "unnecessary" publications into a trash barrel, an action members of Congress and the press labeled book burning.

The original Circular A-130's policy concerning government information dissemination arose out of this environment. Not surprisingly, it conveyed, in tone if not in substance, this message about government information dissemination: when in doubt, don't! The starting point was a negative, almost punitive, attitude toward information dissemination.

When OMB first issued the draft circular in March 1985, a chorus of public criticism greeted its narrow and restrictive view of government information activities. The *New York Times* ran a front-page story with the headline: White House Plans Drastic Cuts in Census Data. It is a mark of the Reagan administration's naivete' in these matters that most of OMB's hierarchy had no idea what document the *Times* article was referring to.

The circular was quickly characterized by public interest groups as stressing private sector prerogatives in disseminating government information to the exclusion of a positive role for federal agencies, and as a document that fostered driving up the price of government information through user charges.

1. Current Revisions to A-130

OMB published its first official revision to Circular A-130 on July 2, 1993, and followed that with a second revision in July 1994.[12] The circular has now abandoned the strong emphasis on the private sector. The original circular carried extensive references to *OMB Circular A-76, Performance of Commercial Activities.* OMB has eliminated almost all those references, although there are still plenty of statements to keep the private sector satisfied. OMB has not repudiated Circular A-76; it simply decided not to advertise A-76 in its IRM policy. In many respects it is a matter of tone and emphasis, but tone and emphasis were among the most offensive aspects of the original circular.

In addition to redressing some obvious deficiencies of the original circular, especially the role of records management and coordination with state and local governments, the circular now devotes much of the information management section to information dissemination. Agencies must set up information dissemination management systems and avoid monopolistic practices, and they are encouraged to disseminate, as well as collect, information in electronic media.

OMB has also tried to respond to criticism that A-130 had no enforcement machinery. The circular now directs that the senior official for information resources management in each agency act as an ombudsman to "consider alleged instances of agency failure to comply with this Circular and recommend or take corrective action as appropriate." Most of the "senior officials" as defined under the Paperwork Reduction Act turn out to be the Assistant Secretaries for Administration, or equivalent, in the agencies. The effectiveness of the ombudsman policy will depend partly on this political appointee's commitment to effective IRM, partly on the amount of power the senior official really wields over subagency program officials, and partly on the official's ability to put the public interest above parochial loyalties. This is a troublesome task for senior officials, most of whom fail to view IRM as anywhere close to the core of their duties. Many agencies say the ombudsman language is simply a restatement of routine responsibilities their agency heads and senior officials have had all along. Perhaps the main thing this policy accomplishes is to place responsibility for responding to consumers' complaints in the agencies' laps rather than OMB's.

---

[12]Office of Management and Budget, *OMB Circular No. A-130, Management of Federal Information Resources*, revised, 58 Federal Register 36068, July 2, 1993; and 59 Federal Register 37906, July 25, 1994.

The circular's Section 8b, Information Systems and Information Technology Management, now leads off with a set of statements about evaluation and performance measurement. Logically, evaluation belongs later in the section, after consideration of strategic information resources management planning, and acquisition and use of technology. OMB puts evaluation and performance measurement first to give them special emphasis. The message to federal agencies is this: it is no longer enough just to do strategic IRM planning; what is important now is to actually measure whether information technology lived up to its plans.

OMB especially stresses benefit-cost analysis of information systems. OMB and the General Accounting Office will collaborate in creating a publication to guide agencies in doing benefit-cost evaluations. In 1992 OMB issued a document entitled *Budget Examining Techniques for Evaluating Information Technology Investments*. The document presented a series of questions to ask when assessing an agency's budget request for information technology systems and contained a discourse on benefit-cost analysis. OMB intends to work with GAO staff to arrive at a consensus revision of this document that both agencies will issue in unanimity.

The revised circular A-130 also codified OMB's new exegesis of reducing the burden an agency imposes on the public. The Paperwork Reduction Act conceives of this "burden" as the amount of time federal agencies force members of the public to spend filling out forms and questionnaires. It is a burden associated with information collection, and under OMB's administration of the Act, each agency is allocated an annual "information collection budget," defined as the aggregate number of hours the agency can inflict forms and record keeping on the public. Now OMB introduces a new meaning of burden. Burden is not only the hours spent filling out forms but also the hours the public spends visiting government offices to acquire information or receive benefits. In the circular's words, "too often, for example, agencies require personal visits to government offices during office hours inconvenient to the public. Instead, agencies should plan to use information technology in ways that make the public's dealing with the Federal government as 'user-friendly' as possible."

However salutary the notion of making government services more user friendly, this meaning of "burden" goes well beyond anything found in the present Paperwork Reduction Act or contemplated for its future amendments. When a federal form is too onerous, a notice at the top of the form invites the public to write to OMB's Office of Information and Regulatory Affairs with their complaint. Presumably OMB investigates these complaints and could revoke the offending information collection's OMB clearance. When government services are unfriendly to users, it is unlikely that OMB will tell the agency to buy a new computer, or move its offices to a shopping mall and stay open on Saturday and Sunday. If an agency starts using smart cards or sets up computerized information kiosks, they will not be able to count that against the mythical five percent burden reduction Congress keeps insisting on.

Greatly minimized in the new A-130 is the doctrine of chargeback for information processing services, the notion that programmatic users of federal computer centers must pay for all computer services. Inspectors general liked chargeback because it was the closest thing the circular offered to a "cookbook" test they could apply when auditing an agency's IRM programs. Where chargeback formerly commanded its own appendix in A-130, the topic is now reduced to a few policy statements with minimal explanation.

The revision does attempt to integrate the twins of IRM, information management and information technology management. In a section on use of information resources, the circular insists that agencies create a management and technical framework to document linkages among mission needs, information content, and information technology capabilities. OMB gives little hint as to what these frameworks should look like. Hopefully, in future issuances OMB will elaborate guidelines concerning how information management and information technology management should mesh to serve agency missions.

2. The IITF Working Group on STI

In August 1994, OMB established a subgroup under the IITF Government Information Working Group to address questions of Circular A-130 implementation in the management of scientific and technical information. OMB specifically invited the agencies represented in CENDI to constitute the group and named Elizabeth Buffum, Director of the Office of Scientific and Technical Information at the Department of Energy, to chair the group. The A-130 Implementation Group is charged with looking at how OMB Circular No. A-130 has been implemented in its member agencies and coming up with a set of best practices in information dissemination management by next March. They are expected to look at their customers' changing expectations and indicate how A-130 has had impact on their internal organization and management. OMB also wants the group to examine interagency cooperation and international issues. At this writing, it is too early to tell what will come from this group.

2. Forecast

Coupled with the 1993 rewrite of information management policy, the new version almost finishes the task of completely rethinking the original A-130 issued in 1985. The chief piece not yet recast is the circular's appendix on computer security, an increasingly thorny political issue because of the White House's commitment and industry's opposition to the Clipper chip. The new circular promises that this final piece is forthcoming. Given the controversy surrounding Clipper, the treatment of computer security may become the last element of controversy in what has become a widely accepted policy document.

In general, the 1993-1994 revisions to A-130 are good news for agencies such as DTIC. The emphasis given to information dissemination in the revised circular provides strong support for DTIC's mission. Modernization and expansion of DTIC's programs are arguably one important way in which DoD can carry out A-130 policies.

E. Federal Records Management

1. PROFS Case and Electronic Records. Are e-mail systems federal records? If everything transpiring on an agency's electronic mail system is legally a federal record, then everything on the system must be preserved. And everything will sooner or later be open to public scrutiny.

These contingencies are real possibilities depending on the final aftermath to *Armstrong v. Executive Office of the President*, the case in which the National Security Archives sued the White House to prevent the destruction of the "PROF" tapes from the Iran-Contra scandal. The PROF tapes were the computer backup tapes for the IRM electronic communications system in the White House. The White House contended the tapes were not federal records because staff were supposed to print out in paper form any information that rose to the level of a record. U.S. District Judge Charles Richey disagreed because the paper record did not show who received the communication and when. Judge Richey found that the White House "record keeping procedures are arbitrary and capricious because there is no adequate management program or supervision by record keeping personnel of the staff's determination of record or non-record status of computer material."

What Judge Richey's opinion means for federal agencies is that, if challenged, they must be able to prove they have established a well defined relationship between e-mail and federal records, and they must be able to show that agency records officers are supervising how staff decide which e-mail messages are records and which are not. Few agencies are in a position to withstand a challenge on these points.

The PROFs case is still dragging on. As a result of the litigation, the White House has now agreed to keep all of its electronic records until the case is resolved. The Center for Electronic Records at NARA is fully occupied with the case and expects to be so occupied for some years to come.[13]

---

[13]Interview with Kenneth Thibodeau, Director, Center for Electronic Records, NARA. Thibodeau estimated his staff might continue to work on nothing but the PROFS case for as much as six years from now.

In the meantime, as one direct outcome of the case, NARA has issued for comment a notice of proposed rulemaking on electronic mail systems.[14] The notice announced that NARA intends to issue general standards under which federal agencies can develop recordkeeping policies and procedures to govern electronic mail systems. NARA was particularly interested in how agencies handle recordkeeping of transmission and receipt information; that is, who originated a message and who received it. They also wanted to know how agencies proposed to monitor their e-mail systems to ensure compliance with recordkeeping obligations.

2. Government-wide E-mail.

The White House wants to develop an electronic mail system within the federal government.[15] The idea is to interconnect government e-mail to public services to improve citizen participation in government. The General Services Administration has now established an e-mail program office in its Office of Emerging Technologies. OMB, for its part, formed an interagency task force to study the creation of an e-mail system for the government. The task force submitted its report to OMB in the spring of 1994, but as of October 1994, OMB had still not issued guidance to the agencies.[16]

F. Federal Printing

In June 1993, President Clinton signed into law the Government Printing Office Electronic Information Enhancement Act. The legislation required GPO to initiate a directory of federal databases, an online access system to the *Congressional Record* and *Federal Register*, and an electronic storage facility. Enactment concluded a two-year process that started with a bill whose original intent was to make GPO the single point of contact for electronic public access to government documents. The law as enacted is much more limited in scope. By summer 1994, GPO had its new service up and running.

The principal effect of this legislation was to provide GPO with a license to produce and disseminate electronic information products. Prior to the act, it was unclear whether GPO's printing laws could be construed to include electronic products which might not comport with a narrow definition of printing. The Act gave GPO

---

[14]National Archives and Records Administration, "Notice of Proposed Rule Making: Electronic Mail Systems," 59 *Federal Register* 13906-13910, March 24, 1994.

[15]John Podesta, Assistant to the President, in a speech at the Freedom of Information Summit, Freedom Forum First Amendment Center, Vanderbilt University, Nashville, TN, April 14, 1993.

[16]Kevin Power, "E-mail Task Force Pushes OMB for a Model Government Policy," *Government Computer News*, October 3, 1994.

authority to enter into electronic publishing and specifically mandated two electronic products.

As part of the National Performance Review, the Clinton administration had announced that it wants to institute federal printing reform. Under H.R. 3400, the legislative package it sent to Congress concerning the NPR, the administration included the "Government Information Dissemination and Printing Improvement Act of 1993." This legislative proposal called for freeing the executive branch from the Government Printing Office monopoly on printing within two years; immediately authorizing executive agencies to buy their own printing services under $2500; establishing the Government Information Locator Service; and coming up with a plan for distributing publications to the nation's 1400 federal depository libraries.

The administration's legislative proposal was politically unrealistic, expecting Congress to remove an executive branch problem whose removal would cause Congress itself the problem of what to do with GPO's 5,000 employees. Not surprisingly, the legislation stalled and effectively died. Other aspects of the proposal also revealed the administration's reluctance to think through the consequences of its reinvention. The proposed bill had little to say about the depository libraries. The bill would have placed the Superintendent of Documents functions into the Library of Congress, a development that the Library did not greet with enthusiasm.[17]

By all accounts, GPO is continuing to lose business and the Joint Committee on Printing continues to fight to save that business. The administration's legislative proposal for federal printing did not pass the Congress. The most recent event in the printing struggles is a memorandum of September 19,1994, from the Director of OMB to the heads of executive agencies.[18] Director Rivlin stated the administration's resolve to accomplish a comprehensive reform of federal printing. That reform should improve the efficient of government printing and duplicating; limit government owned printing to a minimum core capacity; and enhance public access to government information. At the same time, the Director announced that the administration would maintain the *status quo* through fiscal year 1995, and required all executive agencies to procure their printing through GPO.

DTIC is in the same position vis-a-vis GPO and federal printing as other DoD agencies. The presence of the Defense Printing Service serves as a buffer between DTIC

---

[17]The Library of Congress was not a willing recipient of the Superintendent of Documents functions. Internal LOC memoranda indicated the move would be mostly cost to LOC and very little benefit.

[18]Office of Management and Budget, "Procurement of Printing and Duplicating through the Government Printing Office," OMB Memorandum No. M-94-30 for the Heads of Executive Departments and Agencies, September 19, 1994.

and GPO. DPS appears to be fighting successfully for a growing autonomy from GPO, while insisting that DoD is fully committed to using GPO. If the administration succeeds in a legislative revision to the printing portions of Title 44, DTIC will benefit (or suffer) just like other agencies.

G. The GILS Movement.

1. Background

The movement toward a federal information locator system has been alive for at least twenty-five years. The basic concept is that the federal government should have some unified vehicle that the general public could use to locate information among the vast number of publications issued, a finding aid for sifting through the information resources available from the myriad of federal bureaucratic entities.[19]

The concept was first given voice in the proceedings of the Federal Paperwork Commission during the Ford administration. The Paperwork Reduction Act of 1980 (PRA) included language establishing the Federal Information Locator System (FILS) (Title 44, United States Code, Section 3511). Several problems arose from the PRA conception of FILS. A principal difficulty was that the statute defined FILS in such a way as to envision a database whose individual records would consist of data about information *collections*, that is, about forms and questionnaires. Under this definition, FILS would become the database cataloging all the information collections that OMB had approved under the PRA. As a finding aid for locating government publications, FILS was essentially useless. The statutory FILS concept focused on information *inputs* to government, whereas the interests of those needing a finding aid were in the information *outputs* from government.

An additional difficulty was the fact that the PRA charged OMB with responsibility for maintaining and operating FILS. OMB, which conceives of itself as an oversight agency and not an operating agency, never vigorously prosecuted FILS, and settled for a program in name only that was distributed among the principal federal agencies.[20]

---

[19]"A locator is defined as an information resource that identifies other information resources, describes the information available in those resources, and provides assistance in how to obtain the information." See "The Government Information Locator Service (GILS)," Report to the Information Infrastructure Task Force, May 2, 1994, p. 6.

[20]See Gary D. Bass and David Plocher, "Finding Government Information: The Federal Information Locator System, *Government Information Quarterly*, Vol. 8, 1991, p. 11. This article traces the history of the locator concept. The interpretation of events in the text is the author's own, not that of Bass and Plocher,

OMB revisited FILS in 1990 when it commissioned a study by Charles McClure of Syracuse University. McClure advocated abandoning the PRA concept and developing a Government Information Locator Service[21] that would be a true information finding aid. In a second study, McClure introduced the idea of tying GILS to the spreading phenomenon of networks and making agency GILS databases available over Wide Area Information Servers (WAIS) vis the Internet.[22] In 1993-1994, Eliot Christian of the U.S. Geological Survey refined the concept into its current form.

2. The Draft OMB Bulletin

On September 22, 1994, OMB circulated for comment the draft of an OMB Bulletin intended to establish the Government Information Locator Service.[23] OMB intended to decree that all executive branch agencies must establish publicly available inventories of their print and electronic publications in a common format promulgated in a Federal Information Processing Standard that the National Institute of Standards and Technology issues. The FIPS defines a "GILS core," a bare minimum of data elements that each agency must adhere to. Every agency must create a locator database that holds at least the GILS core. The agencies are exhorted to go beyond the core and add more detail and value. The OMB bulletin stipulated not only that agencies must include their information dissemination products in GILS but also the inventory of automated information systems that the Paperwork Reduction Act requires agencies to maintain. Agencies were to have their GILS systems up and running within twelve months of the issuance of the OMB Bulletin.

Also, within 24 months from the bulletin's issuance, agencies were to have submitted to NARA the appropriate records schedules for information resources included in GILS. Although the language here is fuzzy, it appeared that OMB wanted agencies to publish information that would provide inventories of their schedulable records systems, both print and electronic, as well as their print and electronic publications.

---

although they would certainly agree that OMB did not live up to the statutory FILS concept.

[21]McClure coined the name Government Information Locator Service or GILS in order to distinguish his concept from the PRA's concept of FILS. The name GILS has stuck and is now universally used.

[22]Charles R. McClure, Joe Ryan, and William E. Moen, *Identifying and Describing Federal Information Inventory/Locator Systems: Design for Network-based Locators*, 2 volumes, Bethesda, MD, National Audio Visual Center, 1992.

[23]Office of Management and Budget, Memorandum from Bruce McConnell, Chair, Information Policy Committee, Government Information Working Group, to participants at the GILS Public Meeting; Subject: Draft OMB Bulletin; September 22, 1994. The memo announced that comments had to be submitted by October 14.

Public interest research groups, led by OMB Watch, attempted to slow down issuance of the GILS bulletin. (OMB's intent, as reflected in the bulletin's language, was to issue the bulletin in final form before the end of October 1994). OMB Watch and others asked that the comment period for the draft bulletin be extended. These groups want GILS designed in such a way that a given locator entry in an agency's GILS database could become a gateway to the full text of the underlying information resource.

3. Forecast

What will be achieved when a government-wide information locator in place? The important thing is not to do the locator once, but to put it into place in such a way that it continues year after year. That means the locator system must have some intrinsic value to the producer agencies themselves. It should be so intrinsically valuable that, on their own motivation, the producer agencies will find ways to incorporate locator systems into their routine work programs. If the locator is only an externally imposed requirement, -- for example, an OMB bulletin --the agencies will start to drop it as soon as the external pressure diminishes.

Following this line of reasoning leads one to the notion that GILS will have to be viewed by the agencies as an effective replacement for their publications catalogs and directories. In DTIC's case, this could mean that the agency's GILS would be an electronic version of its publication *How to Get It*.[24] The publication would have to be kept current in order to comply with the GILS specification, a budgetary consideration for DTIC to contemplate. On the other hand, DTIC may be in an excellent position to step forward and proffer *How to Get It* as an existing product framework that could become the basis for a DoD-wide GILS. In effect, DTIC could say to DISA: we have already got a GILS product in hand; give us some additional resources and we will fulfill the full GILS requirements for the entire department.

GILS thus becomes both a threat and an opportunity for DTIC. The GILS specifications contemplate that the general public will be able to gain access to an agency's GILS through a network. If an electronic *How to Get It* became the DoD GILS database, DTIC would be stepping into the arena of offering services direct to the public. DTIC needs to evaluate with some care the costs and benefits of seizing the initiative on GILS.

DTIC may also be affected by the provisions of the GILS bulletin that require agencies to publish in GILS a description of their schedulable records systems. GILS

---

[24]Defense Technical Information Center, *How to Get It: A Guide to Defense-Related Information Resources*, Report No. DTIC/TR-92/5, U.S. Government Printing Office, Washington, DC, October 1992.

will, in effect, advertise the existence of these records. While the fact of the existence of some records systems may not have been known in the past, GILS will now advertise the fact. DTIC may well be concerned, as are other agencies, that advertising the existence of records systems will result in a significant increase in FOIA requests which, in turn, could prove sufficiently annoying to DoD components as to cause diminution in the flow of documents to DTIC -- an undesirable outcome. Whether DTIC can take action to mitigate this eventuality is a question that lies beyond this study.

H. The National Information Infrastructure.

Discussions of the National Information Infrastructure have become part of the popular culture of the day. The discussions almost invariably speak of information highways or information superhighways. As a beginning, it will be useful to have a set of working definitions for some of these terms. An *information highway* generally refers to a system of telecommunications pathways and connections that transmits and receives voice, video, and data. An *information superhighway* refers to broadband (high-capacity) telecommunications circuits, increasingly based on fiber optic technology, which can carry much greater amounts of digitized information, such as high-resolution video, at faster speeds. The *National Information Infrastructure* encompasses an integrated web of telecommunications, information, and computing technologies. The vision of the NII is to interconnect businesses, governments, researchers, educators, and the public with advanced communication and information resources throughout the nation.[25]

1. Information Infrastructure Task Force.

In August 1993, the administration announced the establishment of an Information Infrastructure Task Force. The purpose of IITF was to coordinate executive branch policy and implementation efforts in support of the administration's technology policy, Technology for America's Growth: A New Direction to Build Economic Strength, announced in February 1993. The head of the task force was Secretary of Commerce Ron Brown, and it operated under the auspices of the National Economic Council set up by the Clinton White House.

The task force works through three committees:

- **Applications**, chaired by Arati Prabakhar, Director of the National Institute for Standards and Technology (NIST);
- **Telecommunications**, chaired by Larry Irving, Administrator of the National Telecommunications and Information Administration (NTIA);

---

[25]See Virginia Hugh and Stephen B. Gould, "The National Information Infrastructure: The Federal Role," CRS Issue Brief IB93101, Congressional Research Service, Library of Congress, July 11, 1994.

and

- **Information Policy**, chaired by Sally Katzen, Administrator of the Office of Information and Regulatory Affairs (OIRA) in OMB.

The Information Policy Committee, in turn, set up three working groups:

- Government Information, chaired by Bruce McConnell, Chief of the Information Policy Branch in OIRA/OMB;
- Privacy, chaired first by Patricia Faley, Acting Director, U.S. Office of Consumer Affairs; and thereafter by Robert Veeder, initially of OIRA/OMB and now Privacy Advocate for the Internal Revenue Service; and
- Intellectual Property, chaired by Bruce Lehman, Commissioner of Patents and Trademarks.

IITF working groups have issued various reports, particularly as regards privacy and intellectual property, that are discussed elsewhere in this report.

In August 1994, McConnell established a subgroup under the Government Information Working Group to address questions of Circular A-130 implementation in the management of scientific and technical information. (See above, page 2-16.)

I. The Solomons Conferences.

Beginning In 1991, officials in the offices of information resources management in major federal agencies held interagency conferences on public access to electronic government information. The conferences were initially held at Solomons, Maryland, and became known as the Solomons conferences.[26] Five Solomons conferences have now been held, although the venue has shifted to the Washington, DC, area.

Three facets of the Solomons phenomenon deserve noting. First, the major federal agencies, acting collectively, are moving toward activist information

---

[26]The first conference was sponsored by the Environmental Protection Agency in May 1991. The second conference was sponsored by the Department of Agriculture in November 1991. In July 1992, Sprehe Information Management Associates, operating under a contract with the Bauman Foundation, sponsored a public/private sector dialogue in Washington, DC, to critique results to date from the Solomons conferences. The third Solomons conference was hosted by the Department of Commerce in September 1992. The Department of the Interior was the sponsor for the fourth conference in April 1993 in Reston, VA. For a summary of the proceedings of the first three Solomons conferences, see J. Timothy Sprehe, "Issues in Public Access: The Solomons Conferences," *Government Publications Review*, Vol. 20, 1993, pp. 251-272. The fifth conference was held June 27-28, 1994, in Alexandria, VA, under the sponsorship of the Department of Health and Human Services. See *Proceedings of the Fifth Solomons Interagency Conference on Public Access*, Department of Health and Human Services, Washington, DC, September 1994.

dissemination policies. Second, however, the policy output from the Solomons Conferences has remained at a very general level. The conferences have thus far yielded "Public Access to Government Electronic Information: A Policy Framework," (February 1994, U.S. Department of Agriculture); each participating agency, assuming it agrees with the framework, will then use it as an instrument in drafting its own information dissemination policy. The agencies are still perhaps several years away from implementing the policies within agency programs.[27]

Third, the Solomons discussions have highlighted an important reality governing the ability of federal agencies to make their information holdings more accessible to the public. That is, federal agencies have no economic incentives to invest in enhanced information dissemination programs, because dissemination costs must come out of non-budgeted resources. Across the executive branch, agency information program budgets, with few exceptions, do not include funds for making databases accessible to the public, much less rendering them usable and user friendly. Agency budgets will remain tight for the foreseeable future. The Clinton administration's call for making more government information accessible to the public is at present a call to do more with little or nothing. There is no money to apply to expanding existing information dissemination programs, let alone new ones.

Finally, while the early Solomons conferences restricted participation to federal agency personnel, more recent conferences have opened the doors to public interest groups as well. The fifth conference was jointly sponsored by HHS and the American Society for Information Science. Conference organizers have also made substantial outreach efforts to involve a wider audience of federal officials, especially those who staff public affairs offices.

---

[27]Working groups resulting from the Solomons conferences also participated actively in the final design of the Government Information Locator Service, a report on which was presented to the IITF in May 1994.

CHAPTER III

FREEDOM OF INFORMATION ACT

The Freedom of Information Act (FOIA) is intended to be a basic guarantor of openness in government. FOIA provides that the records of government shall be available for access to the public, upon request, at a nominal charge, subject to nine exemptions. To secure copies of records from a federal agency, a member of the public need only write a letter to the agency, citing the Act and identifying the records requested. A statutory formula is provided for waiving and assessing charges.

A. New FOIA Policy in Clinton Administration.

On October 4, 1993, President Clinton issued a memorandum to all executive branch agencies concerning FOIA. Stating his commitment to enhancing the Act's effectiveness, he called on agencies to renew their commitment to the Act's underlying principles of government openness and to embrace new litigation guidance issued by the Attorney General. For her part, Attorney General Reno rescinded the 1981 Justice Department guidelines for the defense of agency action in FOIA litigation.

> The Justice Department will no longer defend an agency's withholding of information merely because there is a 'substantial legal basis' for doing so. Rather, in determining whether or not to defend a nondisclosure decision, we will apply a presumption of disclosure.[1]

The Attorney General strongly encouraged FOIA officers to make "discretionary disclosures" whenever possible under the Act. The Justice Department is undertaking a comprehensive review of all pending FOIA cases as well as FOIA forms and correspondence. She also urged agencies to clear up their administrative backlogs under the Act.

The administration's action on FOIA changed the ground rules. During the Reagan and Bush administrations, the presumption had been that, if public disclosure could be refused under the law, it should be refused. The new rule is that, if disclosure can be granted, it should be granted.

It does not appear that the new ground rules will substantially alter the way agencies conduct their FOIA business; so far it seems like business as usual. In this

---

[1]Letter of Attorney General Janet Reno to Heads of Executive Departments and Agencies concerning Administration of the Freedom of Information Act, Department of Justice, Washington, DC, October 4, 1993.

sense, there may be little real significance, other than as a symbol, to the Clinton administration's new posture on FOIA.

B. Electronic Freedom of Information Act Principles

In mid-1994, an interagency group, chaired by Dan Metcalf of the Department of Justice, completed a draft document entitled something like "Principles of Electronic FOIA." Reportedly, it contained 66 principles that the agencies believed should govern electronic FOIA. The draft was submitted to OMB, and as of October 1, 1994, had not been released by OMB. The draft was intended to be circulated among federal agencies as a proposed administration position on S. 1782 (see below). The author was unable to secure a copy in time for inclusion in this report.

C. Electronic Freedom of Information Act

On November 23, 1993, Senator Patrick Leahy (D-VT) introduced S. 1782, the Electronic Freedom of Information Improvement Act of 1994. Senator Leahy had introduced substantially the same legislation in the past several years. The bill would require agencies to publish indices of their electronic information holdings, to make all regulations available electronically, and to make reasonable efforts to provide information in formats requested by the public.

What does "electronic FOIA" mean? The phrase is usually understood to mean that, if an agency possesses the requested information in electronic format, and if the requester asks for the information in electronic format, and assuming a request does not fall under the Act's exemptions, the agency must provide the information in electronic format. The narrow conservative interpretation followed by many government attorneys during the Reagan and Bush administrations held that, under the FOIA as presently written, the agency has the option to choose the format in which the information is delivered to the requester. Conceivably, under this interpretation, an agency could elect to print out an electronic database on paper and deliver it to the requester in this form.[2] While many FOIA experts believe the Act already covers electronic formats, most agree that the Act would benefit from clarification on this point. At the same time, it should be noted that one hears nowadays of no cases in which agencies are refusing to furnish electronic media when requested to do so under FOIA.

---

[2]And this was sometimes done. The Central Intelligence Agency is one agency where this occurred.

One fear that electronic FOIA has engendered in federal agencies, particularly OMB, is that, were the law clarified, commercial database vendors might be given a license to go shopping through agency databases in search of commercially exploitable databases. If this occurred on a widespread basis, the agencies would conceivably have to devote a great deal of time and money to segregating "FOIAable" from "nonFOIAable" information in their databases. On the other hand, a number of states have had electronic FOIA statutes in place for some years, and one does not hear of major administrative problems encountered by these states.

More fundamentally, these critics argued, the FOIA was intended to promote openness in democratic government rather than to serve as the basis for commercialization of government information. They believed that, before an electronic FOIA bill was passed, the nation needs a thorough debate on the Act's foundations and a means of balancing openness in government against commercial interests. S. 1782 did not treat these arguments. The bill appeared to take the posture that, if FOIA is used to acquire databases for commercial exploitation, so be it.[3]

The bill's primary purpose was to increase public access to government records under the FOIA. It would have required agencies to provide information to requesters in the form requested, by "computer telecommunications" or by other electronic forms such as CD-ROM or on disk. In doing so, it was specifically aimed at *Dismukes v. Department of the Interior* in which the court held that the agency "has no obligation under the FOIA to accommodate plaintiff's preference [but] need only provide responsive, nonexempt information in a reasonably accessible form."[4] The bill aimed to accommodate the requesters' preferences.

Senator Leahy's bill introduced several other ideas to the FOIA. First, under subsection (b)(3) of the Act, agencies would have been able to withhold information that is exempted from disclosure by other statutes. The bill required the agencies to routinely publish the list of such statutes in the Federal Register. Second, agencies would have had to create and publish databases whose contents described FOIA requests the agency has fulfilled (the provision was not retroactive but would begin when the bill became law.). The idea was that the public, as well as the agency, could examine the database and ascertain whether a contemplated request had already been accommodated in the past. Theoretically, this would reduce cost and search time for both the agency and the public.

---

[3]Personal interview with Beryl Howell, Senior Counsel, Subcommittee on Technology and the Law, Senate Judiciary Committee, August 1994. Ms. Howell pointed out that she had heard this objection from OMB, but from no one else, and that she had spent a lot of time speaking with agency FOIA officers.

[4]*Dismukes v. Department of Interior*, 6603 F. Supp. 760 (D.D.C. 1984).

Third, the bill proposed a number of measures to reduce agency delays in responding to FOIA requests. The ten-day response period was extended to twenty days. The agencies could retain half of the fees they collected if their responses were prompt. Agencies would have had to demonstrate why a delay in responding was warranted by circumstances. Agencies were explicitly permitted to follow "multitrack FIFO processing," under which they would separate requests into a simple and a complex track and process them on a "first-in-first-out" basis.

D. "Public Information" versus "Non-Public Information"

In foregoing chapters, the term "public information" has occurred several times. Current efforts to reauthorize the Paperwork Reduction Act used the following definition:

> The term *"public information"* means any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public.[5]

The Information Industry Association uses essentially the above definition in its *Principles for Federal Dissemination of Public Information: An Analysis*, although it shifts the emphasis (see Chapter V). IIA appears to believe that all government information is essentially public information because it is created and processed with public funds; such government information is not made public because of various legal and public policy considerations.

Many gradations can be devised between what is clearly not public information and what clearly is public information. In the cases of the PRA and IIA, those documents deal with information the agency has already made public: holdings in public reading rooms; information disclosed pursuant to the Freedom of Information Act; information the agency makes available on request from the public (without a FOIA request); and information the agency actively distributes as printed or electronic publications.

---

[5]S. 560, "The Paperwork Reduction Act of 1994," §3502 (11).

Public and Non-Public Information

Non-Public Information	Gray Area Non-Public	Public Information
1. Information classsified for purposes of national security. 2. Information withheld because it is **proprietary**; i.e., someone's private property. 3. Information withheld under the **Privacy Act** 4. Information withheld under the 9 exemptions of the **Freedom of Information Act.** 5. Information withheld as specified under some other law.	Information held by agencies that theoretically could be made public but has not been. Reasons: 1. Information of no value outside the government. 2. No one has ever asked for it. 3. Agency does not have resources to make publicly available. 4. No interested party in the public knows the information exists. 5. Information "unfit" to release; i.e., raw data, known to contain errors, incomplete, transitory. 6. Information judged "sensitive" but nonclassified under Computer Security Act. 7. Some combination of foregoing reasons.	1. **Dissemination:** Publications -- electronic, video, printed, or whatever medium -- distributed by government agencies. -Includes information agencies **must** publish; e.g., notice of agency place of business, operations, decisions; public health and safety notices. 2. **Access:** Information disclosed under the FOIA or Privacy Act. 3. **Disclosure:** Public records; information disclosed to the public, e.g., in public reading rooms, pursuant to law or regulation. 4. **Availability:** Information not falling under above 3 categories that agency determines administratively to release to whomever requests it.

The table above represents *one way* of dividing up the information domain into public, non-public, and gray area information; others may devise other ways. Clearly some kinds of information must be withheld from the public, and by the same token some kinds of information must be distributed and even actively broadcast to the public. In between these two extremes lies a broad area of information over which the agency has administrative discretion; the agency can decide for itself whether to withhold or distribute the information.

What has happened over the past 20 years or so is that the gray area may have shrunk. Increasingly, agencies maintain information in electronic formats. When the information is already in electronic format, it is much easier to distribute. The independent regulatory agencies are good examples. When the Securities and Exchange Commission's public records were on paper, no one seriously contemplated the possibility of publishing those records. Gradually over time the SEC itself employed contractors to answer public requests by putting the records in microform and eventually in electronic format. SEC took the dramatic additional step of requiring filers to submit the information in electronic format -- electronic filing. Now that the agency has moved toward full electronic formats, it becomes much easier to disseminate the entire database to the public and to make it electronically searchable.

Moreover, agencies are now required to disseminate to the public information about the *existence* of their record systems. The Privacy Act, for example, requires annual publication of information about systems of records containing individually identifiable information. The more the agencies tell the public about the existence of information, the more opportunity the public has to request access to the information. One outcome of the establishment of GILS [see Chapter 2] will be a formal mechanism for informing the public about the existence of more gray area non-public information. Not surprisingly, some agencies have protested the establishment of GILS precisely on the grounds that they will be administratively burdened with more FOIA requests deriving from GILS.

GILS will also bring about more pressure to move information holdings from the gray area non-public category to the public *dissemination* or at least *availability* category. That is, beyond FOIA requests, the public will petition the agencies to make various databases and other information holdings a part of the agencies' publications programs. The agencies, not foreseeing budgetary resources with which to respond affirmatively to these petitions, are understandably reluctant to see this development occur. What agencies would doubtless like, therefore, would be some policies or even rules of thumb for deciding how to move information resources from the gray area non-public category to either of the other categories. Most policies, including circular A-130, are formulated at a level too general to be of much help in this regard.

E. Forecast

In August 1994, S. 1782 was reported out of the Senate Judiciary Committee and was passed by the full Senate. A companion bill was introduced in the House by Rep. Cantwell. Senate staff were hopeful that the bill would pass in the current Congress. However, House committee staff were less sanguine.[6] They pointed out that it was late in the session; that 1994 was an election year in the House and few were disposed to take up relatively minor legislation that could be controversial. The bill has been around for a number of years and it still has its problems. In the event, the electronic FOIA legislation did not pass the 103rd Congress.

Some Congressional staff doubted that the various incentives S. 1782 carried for speeding up agency action would have the desired effect. They still saw substantial problems with the bill, which in all its versions had been considered rather inartfully drafted.

---

[6]Personal interviews with, among others, Robert Gellman, Acting Staff Director, House Subcommittee on Information, Justice, Transportation and Agriculture, August 1994.

In general, most people think a database listing all FOIA requests the agency has filled would be a useful idea. Agency FOIA officers canvassed by Senate committee staff actually suggested the idea and were said to be strongly in favor of it for internal management purposes. The idea is also one that could be easily incorporated into initiatives for the Government Information Locator System [see above, Chapter II].

Electronic FOIA is a topic that is very likely to arise and to be the subject of successful legislation in the 104th Congress. Both Senate and House staff believe that the climate of opinion is favorable to passage of such legislation, although House staff especially believe that S. 1782 is not a good model on which to build. 1995 could well be the year for reform of the FOIA to include electronic records.

Federal agencies will continue to struggle over the question of what is public information and what is not. Public pressure will continue for making more government information public. The advent of the Government Information Locator Service will exacerbate these questions, particularly with regard to public access to records systems.

CHAPTER IV

INTELLECTUAL PROPERTY

A key issue in the new network environment in which federal agencies increasingly find themselves is the complex of issues surrounding intellectual property. Within DTIC, the wider Department of Defense, and the federal community in general, management of intellectual property is a problem area that everyone will have to address.

A. IITF Working Group Report

When President Clinton formed the Information Infrastructure Task Force in 1993, the Task Force was organized into three committees: the Telecommunications Policy Committee which formulates positions on key telecommunications issues; the Committee on Applications and Technology which coordinates efforts to develop information technology applications; and the Information Policy Committee which addresses the underlying information policy issues for the National Information Infrastructure (NII). Later, a Security Issues Forum was established to assess security needs and concerns. Within the Information Policy Committee, a Working Group on Intellectual Property Rights was designated and chaired by Bruce A. Lehman, Assistant Secretary of Commerce and Commissioner of Patents and Trademarks.

In July 1994, the intellectual property working group issued a preliminary draft of its report, titled "Intellectual Property and the National Information Infrastructure."[1] The report treated first with law, examining the basic legislation for copyright, patent, trademarks, and trade secrets. The main focus of the legal treatment was copyright law. The report moved on to technology, looking at technology for controlling access to protected works, for controlling use of the work, for authenticating the work, and for managing rights in the work. This section ended with the development of technology standards. The report then treated briefly of education, and moved finally to its preliminary findings and recommendations.

The Working Group report concluded that copyright law, as applied to the new situation of the NII, was basically sound although it required certain alterations. The report concentrated on the meaning and ramifications of transmission, which refers to

---

[1] *Intellectual Property and the National Information Infrastructure*, A Preliminary Draft of the Report of the Working Group on Intellectual Property Rights, Bruce a Lehman, Asst. Sec. of Commerce and Commissioner of Patents and Trademarks, Chair, July 1994.

the sending of a copy of a work from one computer to another as, for example, by electronic mail. The Working Group recommended amending the Copyright Act to "reflect that copies of works can be distributed to the public by *transmission*, and such transmissions fall within the exclusive distribution right of the copyright owner."[emphasis added] The Working Group also recommended changes to the definition of "transmit" so as to make it clear that computer-to-computer exchanges fall within the definition and changes to the definition of "publication" to include distribution by transmission. Recommended changes to "importation into the U.S." would also include transmission. The Working Group would amend the "first sale doctrine" to clarify that first sale does not include transmission.

The report noted that technology can defeat any protection technology itself provides. The Working Group would change the Copyright Act to prohibit the importation and manufacture of devices or services that defeat anti-copying systems. The report noted that copyright management information -- name of copyright owner and terms and conditions for use of the work -- may be critical to efficient operation of the NII and recommended prohibiting fraudulent inclusion or removal of such information.

The Working Group was concerned that members of the public have the same opportunities to browse copyrighted works on-line as they now have off-line. The group concluded that it should sponsor a conference that would bring together copyright owners and users in order to develop new guidelines for what constitutes fair use in the NII environment. With respect to

Recommendations of the Lehman Report on Intellectual Property and the NII

1. LEGAL ISSUES

AMENDMENTS TO COPYRIGHT EXCLUSIVE RIGHTS:

- Clarify that unauthorized transmission of a work (e.g., through a computer network) violates the copyright owner's exclusive right to distribute the work (as well as the exclusive right to copy it).
- Broaden the definition of "publication" to include distribution through transmission (e.g., of an online database).
- Clarify that the recipient of a work through transmission (e.g., by downloading from a network) is not free to copy and pass it on without permission.
- Create an exclusive right in public performance of sound recordings in digital formats.
- Don't create any new compulsory licenses.

TECHNOLOGY AMENDMENTS:

- Create criminal and civil liability for importing, manufacturing or distributing technology aimed at circumventing encryption, scrambling, or other copy protection techniques.
- Add criminal penalties for fraudulently creating, removing or altering electronic copyright management information (e.g., a header or software envelope that identifies ownership of intellectual property rights).

FAIR USE:

- Convene a conference of copyright owner and user interests to develop guidelines for fair use of copyrighted works by and in public libraries and schools.

INTERNATIONAL:

- Work for strong national treatment (i.e., no discrimination against foreign copyright owners) and enforcement of exclusive rights under copyright.

2. TECHNOLOGY ISSUES

- No recommendation on establishing encryption or copyright management technical standards, except to allow an owner of intellectual property rights involved in the standards to veto use of its property in the standard.

3. EDUCATION ISSUES

- Convene a conference to develop curricula on intellectual property education, including dissemination of the fair use standards developed by the fair use conference.

licensing, the Working Group was content to allow the market to develop legal licensing systems for the NII.

The Working Group realized that the problems faced in a national information infrastructure would be repeated and doubtless magnified in a global information infrastructure (GII). Here the Berne Convention is a subject of controversy, particularly as regards the scope of the national treatment obligation (see below). Rules must be formulated in the international arena as well as the national, based on the following principles:

1. Each country participating in the GII shall accord to nationals of other participating countries no less favorable treatment than it accords its own nationals with regard to rights and benefits.

2. Benefits shall include the same possibility to exploit and enjoy rights in the national territory of a participating country as the country grants its own nationals.

3. No participating country shall require rights holders to comply with any formalities as a condition of according national treatment.

The Working Group concluded that international protection will depend on resolving differences between the continental *droit d'auteur* rights systems and the Anglo-American copyright systems.

With respect to technology, the Working Group noted the importance of the technology standards process, although that process lay outside the group's purview. Finally, the Working Group concluded that effective public education about intellectual property rights is crucial to the success of the NII. Following its conference on fair use, the Working Group would sponsor a conference on intellectual property education in order to develop school and library curricula.

B. An Industry Framework for Managing Intellectual Property

A more sharply focused viewpoint regarding intellectual property on the NII comes from a recent industry publication. In March 1994, the Information Industry Association published a monograph by Joseph L. Ebersole, titled *Protecting Intellectual Property Rights on the Information Superhighways*.[2]

---

[2]Joseph L. Ebersole, *Protecting Intellectual Property Rights on the Information Superhighways*, Information Industry Association, Washington, DC, March 1994.

One of the challenges facing DTIC in the new network environment is managing intellectual property. Ebersole suggests that eleven elements are necessary in developing a framework for the management of intellectual property. The elements are:

1. A means for identifying a work and its copyright status.
2. A means for assuring that conversion of the work into digital form will include the work's identity, its copyright status, and whether permission for conversion has been granted.
3. A means for authenticating each work.
4.. A means for protecting the work so that only the authorized recipient can receive it.
5. A means for controlling and setting limits on specific uses of the work.
6. A means for "write-protection" of each work against alteration.
7. A means for measuring or metering usage of the work.
8. A means for electronic contracting for access to and use of the work.
9. A means for billing and collecting payment.
10. A means for establishing the parameters of authority for software agents.
11. A means for assuring that the copyright identification and means of control stay with every portion of the work when it is downloaded or printed.

Another way to approach the question of managing intellectual property is to survey briefly the management practices of in use by vendors in the private sector. Examples come from the vendors of online databases such as Lexis, Westlaw, Prodigy, CompuServe, America OnLine, and so forth. These firms typically handle access by granting their customers a nonexclusive, nontransferable limited license to access their databases. Their agreement always cover rights to download from their systems, although they vary as to whether they permit any downloading and how much. Typically they sets limits on the use of downloaded data such as internal use only or no inclusion in the customer's searchable databases. Printouts are also restricted to internal use. Vendors do provide gateways to other services. When the service provides access to third party databases, customers are responsible for complying with the terms stipulated by the owners of the databases. Some vendors provide document delivery services for longer full text documents. The firms usually have special agreements for information brokers in order to allow them to provide output to their clients. Consumer oriented services use less formal agreements, sometimes referred to as "click-wrap" in which the act of enrolling in the service is defined as the act of acceptance of the conditions of membership; transmission of the customer's credit card information is included in the acceptance act.

As regards commercial publishers of CD-ROMs, publishers almost always use agreements that license the databases rather than selling them outright. The reason for

licensing is that, if sold, the databases could presumably be resold by customers under the first sale doctrine, an outcome publishers wish to avoid. The contents of CD-ROMs are often dynamic, changing frequently; hence they are complex products containing both software and databases. CD publishers require flexible pricing schemes that permit both flat fees and usage based fees. Ebersole reviews three commercial pricing systems: CD-MAX, the Wave system, and InfoSafe Systems.

Another area in which commercial vendors have developed intellectual property management applications is software licensing in network environments. The Microcomputer Managers Association and the Society for Information Management have issued white papers outlining software licensing issues and problems. Several techniques have been developed to deal with software licensing. One is the "license manager" which stores copies of software on a server along with the names and passwords of approved users. The server releases a copy of the software to the approved customer while the product is being used, and then checks the copy back in after usage. Limiting the number of copies available from the server rations usage among customers. License managers have obvious applications in the library setting. Another technique is "superdistribution" which requires a microchip installation in a PC or LAN server. The chip protects a distribution and payment system in an open network environment such as the Internet.

In the electronic environment, methods are being developed for protecting intellectual property. In particular, the concept of "envelope" is being elaborated for this purpose. The idea is that a particular electronic work is put into a software "sealed envelope" whose contents are sealed and hidden by encryption. The envelope has displayable information on the outside such as title, author, publisher, copyright notice, abstract, and keywords. Objects in sealed envelopes are processed by "rendering software" obtained from the work's authorizing distributor. Once the user's identification and password are certified, the user is permitted to open the envelope and use the contents. Other systems use the concept of "header" with identifying and copyright information embedded in a header attached to the electronic work.

The foregoing descriptions serve to emphasize the point that various solutions, however piecemeal, are already being applied to problems of intellectual property management. DTIC may wish to study this rapidly changing phenomenon to discover whether others have already devised management strategies that DTIC could adopt.

C. Software Copyright

One of the areas in which the policy interests of STI agencies may diverge from those of other information programs and agencies is copyright protection for computer

software.[3] In recent Congresses, several efforts have been made to legislate a limited government copyright for federally generated software to enhance technology transfer. OMB's Office of Information and Regulatory Affairs, the home base for OMB Circular No. A-130, has generally taken the view that any government copyright is an undesirable change in the Copyright Act. OMB sees the movement toward software copyright as the thin end of a wedge that would lead to greater and greater assertion of federal control over the uses of government information.

The STI agencies, on the other hand, operate under the Federal Technology Transfer Act of 1986 which enjoins them to benefit the general public by transferring the fruits of federal research and development to the private sector. The Act established the CRADA: Cooperative Research and Development Agreement. CRADAs are negotiated between federal agencies and private parties and are a vehicle for transforming federally generated intellectual property into commercially marketable products and services. CRADAs are effective in encouraging the transfer of patentable hardware and other inventions to commercial exploitation but no analogous process exists for computer software. Private firms have little incentive to develop commercially viable software from government software if they cannot protect their investments through copyright. Hence the STI agencies are among those who argue that Congress should enact legislation providing limited copyright for federally developed software.

D. Open Source Intelligence and Copyright

The federal government's intelligence agency community, facing smaller budgets for the foreseeable future, has begun in recent years to explore more actively ways for sharing information across agency boundaries.[4] Where two agencies cover the same area of intelligence gathering and analysis, the agencies are investigating the possibilities for having only one agency operating with agreements to share the results among other interested agencies. This movement entails both securing the information more quickly and disseminating it more quickly in the light of contemporary information technologies. Under the current working arrangements, for example, agencies are finding that it takes them as much as six months to make conference proceedings available beyond the original analyst.

---

[3]See, for example, Kent Smith, Deputy Director, National Library of Medicine, "Copyright Protection for Computer Software to Enhance Technology Transfer," testimony before the House Subcommittee on Intellectual Property and Judicial Administration, Committee on the Judiciary, May 6, 1992.

[4]This discussion is based principally on an interview with Paul Ryan, Deputy Director, DTIC, October 5, 1994.

Of particular interest is so-called "open source" intelligence, information that can be freely gathered or purchased by anyone with the means to do so. The intelligence community estimates that perhaps as much as 40 percent of their information is open source in nature.

As the agencies investigate sharing across agency boundaries, they have discovered problems of incompatible systems that inhibit sharing. One solution to these problems, particularly as regards open source intelligence, is to use a single common agency as a repository and central distribution point for the information. Hence the agencies have turned increasingly to DTIC as a kind of clearinghouse or communications node. The intelligence agencies could ask DTIC to accession their information holdings and then interested members of the community could draw the information from DTIC. DTIC already possesses the desired infrastructure for sharing information.

Traditionally, the intelligence agencies have shared information only within agency walls or among the community, but not beyond federal agency boundaries. This is now changing and the Foreign Broadcast Information Service is a case in point. FBIS is operated by the Central Intelligence Agency and contains thousands of foreign sources. CIA has now established a memorandum of understanding with the National Technical Information Service to make FBIS output available outside the federal government. Other elements of the intelligence community are actively considering making their open source intelligence available to the general public. The impetus for this movement is found partially in the efforts to reinvent government and partially in the desire to justify intelligence activities in the climate of diminishing resources in the post-Cold War era.

In this new atmosphere of openness, the intelligence community is concerned about problems of copyright. Intelligence agencies collect open source intelligence and are contemplating dissemination of this intelligence to the public. So long as the agencies summarize their sources and share within the federal government, no copyright problems arise. To the extent, however, that the agencies redisseminate whole works to the general public from their open source holdings, they will encounter problems of copyright, especially as regards the Berne Convention.

In March 1989, the U.S. joined the Berne Union by signing a treaty called the Berne Convention, whose full name is the Berne Convention for the Protection of Literary and Artistic Works.[5] At the same time, the U.S. modified its copyright law to

---

[5]See Copyright Office, "The United States Joins the Berne Union," Circular 93a, February 1989, Library of Congress, Washington, DC. See also Copyright Office, "Highlights of U.S. Adherence to the Berne Convention," Circular 93, August 1989, Library of Congress, Washington, DC.

satisfy obligations under the treaty. The effect of the Berne Convention is that all 79 signatory nations agreed that copyright in authors' works will be automatically protected both within their boundaries and internationally. The U.S. and other members agreed to treat nationals of other countries like their own nationals for purposes of copyright. One additional effect is the abolition of a mandatory notice of copyright for published works. Failure to place a copyright notice on copies of published works no longer results in loss of copyright.

For U.S. Federal agencies dealing in international STI, the impact of joining the Berne Union is that the agencies must presume all open source information from other countries is copyrighted. So long as such information was intended only for agency internal use, this presented no problem. As intelligence agencies have begun discussing dissemination of open source intelligence to the general public, the agencies are threatening to run afoul of the Berne Convention.

DTIC disseminates some international STI through NTIS. NTIS intends to accept responsibility for administering copyright in selling these STI holdings. NTIS will establish a set-aside escrow fund into which a portion of the sales price will be deposited and NTIS will pay royalties to copyright holders from this fund.[6]

These problems are under active consideration by the Interagency Gray Literature Working Group. Grey literature is information that is not readily available through routine publishing sources, such as conference and workshop proceedings. IGLWG is developing a strategy paper for its members.

DTIC itself has already adopted certain steps to handle the copyright problem. The first step DTIC takes with respect to a user's request, is to ascertain if the work in question is marked as copyrighted. If it is, DTIC will go get the document, paying the purchase pricing including royalty, and pass on the work to the user. In this respect, DTIC serves as the user's acquisition agent. If the work is not marked with copyright, DTIC will then approach the work's publisher and negotiate acquisition from the publisher. If neither of these avenues proves fruitful, DTIC will try to find out who owns the copyright and approach this party with the request. DTIC will also maintain a record to consult in the future concerning the work's copyright ownership.

---

[6]Interview with Don Johnson, Director, National Technical Information Service, Department of Commerce, April 21, 1994.

E. Forecast

Issues surrounding intellectual property will continue as one of the "hot" areas in federal information policy. It is clear that one of the major question marks affecting commercial development of the network environment is whether private sector interests can feel confident that their intellectual property will be safeguarded on the network.

DTIC will continue to need a framework for managing intellectual property within its own operations. Commercial developments in the framework area are now appearing with some frequency, but it remains to be seen whether these developments will transfer well into the federal environment. The growing tendency of intelligence agencies to provide open source intelligence to the general public will increase the demand for workable management guidance.

STI agencies will continue to press for some limited copyright for government generated software, as an important link in technology transfer. OMB's OIRA will continue to oppose this action. The conflict will be resolved either by legislative action or the development of genuine government-wide STI policy.

CHAPTER V

INDUSTRY VIEWPOINT ON FEDERAL INFORMATION DISSEMINATION

A. Introduction

The Clinton administration's upbeat attitude toward information technology has sparked substantial responses from the private sector. For example:

- **The Computer Systems Policy Project**, representing the chief executive officers of the 13 major U.S. computer companies, released "Principles for a National Information Infrastructure," and "Perspective on the National Information Infrastructure."

- A group of local and long-distance telephone company chief executive officers submitted their own joint statement on information infrastructure to a Congressional hearing in March 1993.

- **The Council on Competitiveness**, representing major companies, labor unions, and universities, issued a report in May 1993 on a *Vision for a 21st Century Information Infrastructure.*[1]

- In July 1993, the **Information Technology Association of America** issued a paper on *National Infrastructure: Industry and Government Roles.*[2]

- **The Coalition for Networked Information** issued a "Proposed Networking and Networked Information Agenda for the Clinton Administration." CNI is mostly oriented toward academic computer and data users and their libraries. CNI also issued in 1993 a proposal for an "Access to Public Information Proposal (APIP)" which was heavily reliant on Internet.

- **The Electronic Frontier Foundation** presented testimony on communications infrastructure issues and also circulated a draft paper entitled "Needed: New Federal Information Dissemination Policy and

---

[1]Council on Competitiveness, *Vision for a 21st Century Information Infrastructure*, Washington, May 1993, 25 pages. See also, Council on Competitiveness, *Competition Policy: Unlocking the National Information Infrastructure*, Washington, December 1993, 31 pages.

[2]Information Technology Association of America, *National Information Infrastructure: Industry and Government Roles*, Arlington, VA, July 1993, 23 pages.

Programs." EFF has also been a major player in the developments surrounding the Clipper chip -- EFF chairs the public interest and industry coalition working to defeat Clipper -- and in defining the administration's positions on the information superhighway. EFF has also played a key role in the digital telephony legislation.

B. The Information Industry Association

Finally, and perhaps most directly germane to this report, the Information Industry Association has completed its own statement on federal information dissemination policy.[3] Titled *Principles for Federal Dissemination of Public Information: An Analysis*, IIA's white paper is intended as a policy framework based on three tenets. First, federal government information is *public* information, and the Freedom of Information Act has created a broad right of access to government information. Second, the federal government should not discriminate in information dissemination; dissemination should be on equal terms to all.[4] Third, restrictions on the use, reuse, or resale of public information are "antithetical to the goal of widely disseminating government information." That is, democratic governments should not control how public information can be used or decide who may use it.

> The common theme underlying these tenets is that the federal government should encourage the greatest feasible diversity of sources of public information. The goal of federal information dissemination should be to help make public information maintained by agencies more available to citizens. An essential means of ensuring the widest dissemination of public information is to encourage a diversity of providers of that information. A diversity, rather than a monopoly, of information sources best serves the public interest. The public is not served when the government, or some other provider is the only source of public information.[5]

---

[3]Information Industry Association, *Principles for Federal Dissemination of Public Information: An Analysis*, a draft white paper prepared by Ronald L. Plesser and Emilio W. Cividanes, Information Industry Association, Washington, DC, August 1994. At this writing, the IIA white paper is still in draft form. However, it is expected that the paper will be formally adopted as an IIA policy statement during the association's annual convention in October 1994.

[4]For those who follow these matters closely, IIA distinguishes between "equal" and "equitable." Equal means the same, dissemination on the same terms to all. Equitable means fair, dissemination on fair but not necessarily equal terms. Equitable dissemination, for example, admits the possibility of giving some groups more favorable terms than others.

[5]Information Industry Association, *Principles for Federal. . ..*, p. 3.

IIA's principles, which flow from the above tenets, are as follows:

I. **The federal government has a responsibility to ensure broad access in public information.**

A. The federal government should use proven information technologies to provide public access to public information.

B. Public access to public information should apply equally to all information regardless of the media in which it exists.

C. If the government maintains a government information locator service, the service should identify private sector as well as public sector products and services containing public information.

D. If an agency offers a data base dissemination product or service to any segment of the public, the government must ensure that the data base underlying the product or service is made available to the public.

II. **Agencies should target their scarce resources to disseminate information products in common, versatile formats to meet unmet needs.**

A. Individual agencies, rather than a centralized governmental authority, should make the decisions to create, expand, or discontinue agency dissemination activities.

B. An agency should make its decisions to create, expand, or discontinue significant dissemination activities subject to public notice and comment, and should provide a written explanation for each such decision.

C. An agency must ensure that its dissemination of public data and of tools used to access the data either is required by law or is necessary for the proper performance of the agency's functions.

D. An agency should not use scarce resources to disseminate an information product that has the likelihood of duplicating other current or future products in the market that reasonably achieve the agency's dissemination objective.

III. **The federal government should encourage the greatest feasible diversity of source of public information.**

A. The federal government should broaden the channels of distribution for public information.

B. The constitutional principle of non-discrimination requires that public information held by a government entity should be disseminated to the public on an equal and timely basis.

1. The government must avoid favoritism and arbitrariness in the dissemination of public information or the use of government information as a commodity of exchange.

2. No agency may establish an exclusive, restricted, or other distribution arrangement that interferes with timely or equal availability of public information to the public, except as specifically authorized by law.

C. Agencies shall not restrict or regulate the use, resale, or redissemination of public information products or services by the public.

1. Governmental assertions of control of the public's use of public information run afoul of the centuries-old principles ensuring the free flow of information.

2. Government imposition of fees or royalties for resale or redissemination of public information is a means of governmental control and should be prohibited, except as specifically authorized by law.

D. Agency fees for information should not exceed the marginal cost of dissemination, nor should they be based on usage or redissemination unless such use increases marginal costs.

1. Making public information available at marginal cost pricing encourages its widest dissemination.

2. Fee-funded agency dissemination operations can diminish public accountability by removing Congressional oversight.

IV. **The federal government should implement its information dissemination policies through a meaningful, open, and workable compliance and review mechanism.**

A. Every agency must designate a specific individual to be responsible and accountable for decisions concerning information dissemination.

B. Every agency must have available an appeal or review mechanism for interested outside parties who wish to seek review of a particular agency decision that is inconsistent with federal information dissemination policies.

The IIA principles are generally consistent with circular A-130, although they add specific emphases that highlight commercial interests. The IIA concept of public information may be overly broad, because clearly much of what IIA would consider public information is not public. Also, principle I-C, the notion that a government locator service must include private sector sources, is something with which most agencies would not agree.

CHAPTER VI

STI AND FEDERAL INFORMATION POLICY

A. Government Information "versus" Scientific and Technical Information

When the Office of Management and Budget published the original version of *OMB Circular No. A-130, Management of Federal Information Resources* on December 24, 1985, the *Federal Register* notice included a discussion of comments received from the public in response to publication of the draft circular on March 15, 1985. When treating of the definition of the term "government information," the discussion had this to say:

> Several commentators recommended that government information be subdistinguished, with special definitions being formulated for, and special policy treatment given to, scientific and technical information, statistical information, or printed information. OMB did not accept the recommendation because the Circular is intended to implement the Paperwork Reduction Act, and the Act itself does not distinguish among various kinds of information.[1]

In the various intra- and inter-agency forums where Circular A-130 was considered, the question repeatedly arose: what is the relationship between "government information," on the one hand, and [government] "scientific and technical information" (STI) or [government] "statistical information," on the other? The answer that OMB staff offered to this question went along the following lines:

- Government information is the most general and all encompassing term. All STI and statistical information created by federal agencies is government information, but not all government information is STI or statistical information. Government information is the "set," and STI and statistical information are "subsets" of government information.

- In preparing Circular A-130, OMB was articulating federal information policy at the most general level, and OMB believed that Circular A-130's policies were applicable to federal STI and statistical information.

- At the same time, OMB believed that special policy issues exist with

---

[1]Office of Management and Budget, *Management of Federal Information Resources; Final Publication of OMB Circular No. A-130*, 50 *Federal Register* 52731, December 24, 1985. As the ensuing discussion implies, OMB would accept some distinctions pertaining to scientific and technical information and to statistical information, but would in all probability not agree that "printed information" is meaningfully different from other kinds of government information.

respect to STI and statistical information. Over and above the policies set forth in Circular A-130, it will be necessary, from time to time, to develop special policies that apply to government STI or government statistical information, but do not necessarily apply to all government information.

B. Statistical Policy Directives

This distinction between government information as the whole and government STI/statistical information as the part has been recognized in practice for many years. OMB's Statistical Policy office issues "Statistical Policy Directives." These directives, which in OMB's view have the force of OMB circulars, pertain to federal statistical information only.[2] The current list of Statistical Policy Directives is as follows.

Directive No. 1.	Standards for Statistical Surveys
Directive No. 2.	Standards for the Publication of Statistics
Directive No. 3.	Guidelines for the Release of Principal Federal Economic Indicators
Directive No. 4.	Prompt Compilation and Release of Statistical Information
Directive No. 5.	Standard Reference Base Period for Federal Government General-Purpose Index Numbers
Directive No. 6.	Standard Federal Administrative Regions
Directive No. 7.	Standard Metropolitan Statistical Areas
Directive No. 8.	Standard Industrial Classification of Establishments
Directive No. 9.	Standard Industrial Classification of Enterprises
Directive No. 10.	Standard Occupational Classification
Directive No. 11.	Standard Data Source for Statistical Estimates of Labor Force and Unemployment
Directive No. 12.	Standard Definition of Payroll Periods for Employment Reports
Directive No. 13.	Standard Data Source of Total Population Used in Distributing Federal Benefits
Directive No. 14.	Definition of Poverty for Statistical Purposes
Directive No. 15.	Race and Ethnic Standards for Federal Statistics and Administrative Reporting.
Directive No. 16.	Standard Classification of Fields of Science and Engineering
Directive No. 17.	Standard Gas Pressure Base
Directive No. 18.	Providing of Statistical Information to International Organizations

---

[2]Statistical policy directives were originally embodied in OMB Circulars No. A-46, A-39, A-65, and A-91. During the Carter administration, the Statistical Policy Division was reorganized out of OMB and placed in the Department of Commerce where it was known as the Office of Federal Statistical Policy and Standards. Since statistical policy was no longer in OMB, its policy statements were renamed as statistical policy directives. The Paperwork Reduction Act of 1980 placed statistical policy back in OMB in the Office of Information and Regulatory Affairs.

OIRA's Statistical Policy branch has continued to maintain the statistical policy directives. At present, OIRA's Chief Statistician is considering a broad revision and reissuance of the statistical policy directives and the revision would take the form of an OMB Circular. [Personal communication from Katherine K. Wallman, July 1994.]

Directive No. 19. Reports of the Department of Commerce on International Transactions.[3]

Government statistical information, then, has its own subset of information policies that pertain to the particular issues affecting federal statistics. These policies are important and dynamic. The Standard Industrial Code, for example, which was revised and reissued during the 1980s, is one of the Government Printing Office's best sellers inasmuch as SIC codes are used throughout government and industry. Directive No. 15 on race and ethnic statistics is a key policy document for monitoring the nation's progress in overcoming racial and ethnic inequality; the directive has been controversial in the past and faces controversy again as plans for the decennial census of population for the year 2000 are drawn up.[4]

Federal statistical agencies produce the principal economic and social indicators, periodic statistics that are considered vital measures of the nation's economy and wellbeing. Some of these statistical measures are based in law and their production is shrouded with official secrecy to prevent manipulation of the numbers for personal gain or political purposes. As Janet Norwood has put it:

> More and more, statistics have become an integral part of public policy. Data series are used to index entitlement programs, to allocate federal funds to states and local areas, and to trigger programs on or off. Statistical series are used for macroeconomic decision-making and for microeconomic programs. They are used by the people of this country to evaluate the effectiveness of their government. We have indeed become a country that is run by numbers.[5]

C. Other Ways of Classifying Government Information

There are many ways of classifying government information. Kurt Molholm has suggested grouping government information into the following classes: consumer

---

[3]U.S. Department of Commerce, *Statistical Policy Handbook*, Government Printing Office, Washington, DC, May 1978.

[4]For a current account of controversies surrounding Directive No. 15, see article in *New Yorker* magazine in July 1994. The essence of the controversy is that some groups identify themselves as "multiracial" and want a multiracial category to be used on the 2000 Census. Traditional racial and ethnic groups believe use of a multiracial category would dilute their numbers and hence their political clout. The article makes the point that the attempt to define racial and ethnic groups in federal statistics for purposes of ameliorating discrimination sometimes has the undesired effect of setting these groups off from others and hence perpetuating discrimination.

[5]Janet L. Norwood, "Statistics and Public Policy: Reflections of a Changing World," presidential address before the 1989 annual meeting of the American Statistical Association, *Journal of the American Statistical Association*, March 1990, Vol. 85, p. 4.

information, citizen information, administrative (or operating) information, business information, and STI. Molhom defines these classes as follows.

- *Consumer information* is government information prepared with the individual citizen or groups of citizens as the intended audience and may be made available through government (and private) organizations that have been established to directly serve the general public.

- *Citizen information* is government information that informs citizens about the operations of their government; it may have been specially prepared to meet the needs of the specific government organization but is available for all citizens.

- *Administrative (or operating) information* is government information used to meet the needs of the specific government organization including that information required for informed decisions making; information of this type is not normally prepared with release to the general public in mind.

- *Business information* is government information such as data, documents, or indices or directories to data or documents that either result from research and data gathering conducted by or for the federal government, or information collected or created by or for federal agencies as part of the business and economic knowledge base for use in federal policy making and regulation and for business planning by commercial firms.

- *Scientific and technical information* is government information that derives from basic and applied research results of scientists and engineers; data, documents, indices or directories to data or documents that either result from research and development conducted by or for the federal government or are collected or created by or for federal agencies as part of the knowledge base for scientific disciplines, technical specialties, and science and technology policy making.

The above elaboration serves to highlight that what distinguishes STI is its relationship to the federal scientific and technical research and development (R&D) process and enterprise. The categories are not mutually exclusive. Some business information is STI. Administrative or operating information can be transformed into citizen information.[6]

---

[6]See, for example, J. Timothy Sprehe, column in *Federal Computer Week*, July 1991, concerning the Transaction Records Analysis Clearinghouse. The column deals with the work of David Burnham and Susan Long. Burnham and Long use administrative information, obtained under Freedom of Information

In Molholm's analysis, the gradations of government information are distinguished by whether or not they require further processing in order to be understandable and useful to the general public. As one moves from consumer information to STI, more processing is needed to make the information humanly understandable and useful. Consumer and citizen information are intelligible to the public by design and definition. Business information and STI, at the opposite end of a continuum, require transformational processing by scientific and technical specialists before the ordinary citizen can use them. In other words, specialists, operating in either the public or private sectors, intervene to turn business information and STI into consumer and citizen information. In part, Molholm's distinctions depend on the *intentions* of the information producers as to who shall be the information users.[7]

D. How STI Is "Different"

The attempt to create a sound analytic distinction between government information in general and STI in particular is a fruitless enterprise. No one has yet devised a good analytic distinction between the two and the effort seems not worth the trouble. Rather, the more useful way to think about the distinction is this:

> Are there important areas of information law and policy that pertain specifically to STI and are inadequately treated in general information policy?

If the question is answered in the affirmative -- as it should be -- one concludes that STI confronts special policy issues that do not necessarily pertain to the rest of government information. One then asks what those special policy issues are.

Act requests, to analyze how the Internal Revenue Service and the Department of Justice are administering the tax and criminal laws; they publish their findings in an effort to make the administration of federal laws more open and evenhanded.

[7]In a different context, the author has suggested even more complicating factors. His thesis, in short, is that an agency's public access is a set of relationships between information producers and information users, and that these relationships change over time, evolving from initial stages of mutual unfamiliarity and suspicion to later stages of relatively symbiotic interdependence. Particularly in the case of agencies specializing in STI, relations between producers and users may be said to be at advanced stages, involving specialized user groups that have highly specific and sophisticated information needs. These people tend to know exactly what they want in terms of public access to government information. They are knowledgeable about the federal agencies possessing the information. They get their information direct from agencies or from a "trade press" that follows the inner workings of the agency. These user groups tend to be highly organized. They tend to use information in high-tech media such as computer tape, CD-ROM, or online; and they are technologically sophisticated and computer literate. See. J. Timothy Sprehe, "Issues in Public Access: The Solomons Conferences," *Government Publications Review*, Vol. 20, 1993, pp. 251-272. See also above, Chapter 3, "Public Information" versus "Non-Public Information."

One way to answer this question is to examine the polarized organizational and cultural setting in which STI exists. STI is pulled in contrary directions by its polarized setting.

At one pole is the *culture of science and academia*, because much of the government's STI is generated by scientists in the nation's colleges, universities, and research institutes. U.S. scientific and academic culture generally places a high value on the uninhibited flow of information. Science progresses best, it is believed, when information is widely shared; hence, barriers to the uninhibited flow of information are counterproductive to the goals of science and the general pursuit of academic knowledge. Scientific and academic culture maintains an imperative in favor of the widest possible dissemination of information. The imperative is much stronger than the broad injunction to government agencies that they should keep the public informed of their doings. In scientific and academic culture, the very reason for creating information is its dissemination (and not, as in most government agencies, the execution of government programs).

At the other pole is the *culture of classified information and export controls*. Within the culture of information classified for purposes of national security, widespread dissemination of information is taboo; the criterion for distributing information is a demonstrated "need to know." Within the culture of export control, certain kinds of information are prohibited from export from the United States except under stringent conditions. These cultures are characterized by an imperative favoring containment of information; the fewer people who have access to information, the better.

Far more than other kinds of government information, STI lives with the dilemma of having to exist in both of these cultures. The government STI community needs policy guidance on how to walk the fine line between the two cultures.

Moreover, the nature of science today is to be *international* in scope, not regarding national boundaries. Indeed, many would argue that one cannot successfully do scientific activities today unless one works at the international level. There is simply too much scientific activity going on in other countries for scientists to remain cloistered behind national boundaries. If one thinks of phenomena such as global warming or acid rain, it becomes clearer that STI, by its very nature, must be international in scope. One consequence of the international nature of STI is that STI policy is to a considerable extent intermixed with and affected by *foreign policy*. International data exchange agreements are often dealt with in treaties or similar foreign policy documents. In this respect, STI is in a far different situation with respect to federal information policy than are most federal information activities.

E. A Policy Circular for STI?

Clearly, in the case of federal statistics, issues have arisen over the years that required a general policy solution directed at a subset of federal agencies and programs. Is the same true for STI? Are there policy issues affecting government STI that are not adequately treated by Circular A-130's general information policy?

The answer is certainly yes. The environment in which STI lives has distinctive policy issues that do not pertain to all government information. As a beginning, one can list at least the following:

1. Policies Directly Applicable

Federal Research and Development Policy. STI programs fall within the boundaries of federal research and development programs. The broad policies affecting federal R&D are applicable to STI. The current policy leanings with respect to federal R&D are in the direction of setting priorities and sharing of functions and resources across agency boundaries. This development is already affecting DTIC in terms of the newly voiced interests of intelligence agencies in using DTIC as an integral link in new information distribution arrangements.

Technology Transfer Policy. The U.S. Government has a set of laws and policies pertaining to the transfer of federal technology to private industry. These laws and policies are directly applicable to STI.

Technology transfer is a means for getting federally generated technology and expertise to the business community where it can be developed, commercialized, and made use of by the public. Technology transfer laws and policies actually present some direct *conflicts* with federal information policy as found in OMB Circular A-130. For example, A-130 would have the agencies disseminate the results of federal R&D in a timely fashion on equal terms to all. The Federal Technology Transfer Act, on the other hands, permits GOCOs -- government owned, contractor operated laboratories -- to enter into Cooperative Research and Development Agreements (CRADAs) with private sector parties. Among the terms of CRADA is the stipulation that the private sector party shall have exclusive use of the R&D results for a period of five years.[8] During that time, the government does not even receive a copy of the results. The CRADA policy would appear to conflict directly with the A-130 policy.

---

[8]This discussion is based on an interview with Elizabeth Buffum, Department of Energy, October 4, 1994.

Another conflict occurs over the question of government software copyright. STI agencies, pursuing technology transfer policies, favor a limited government copyright on software. The information policy staff in OIRA/OMB, keepers of A-130, are adamantly opposed to software copyright.

2. Policies Indirectly Applicable

Information Classified for Purposes of National Security. The U.S. Government has a set of laws and policies pertaining to classified information. Far more than the general run of government information, STI exists in and frequently rubs up again the world of government information classified for purposes of national security.

Export Control Information. The U.S. Government has a set of laws and policies pertaining to the export of certain critical technologies. Far more than the general run of government information, STI by its very content falls into the category of export controlled information.

3. Policy Areas Omitted from OMB Circular A-130 but Important to STI

International Information. Circular A-130 chose to concentrate on the management of federal information resources to the *exclusion* of international information. The most that Circular A-130 does is to include, under Basic Considerations and Assumptions, the following obvious and innocuous statement:

> §7m. Federal Government information resources management policies and activities can affect, and be affected by, the information policies and activities of other nations.

Far more than the general run of government information, STI falls into the category of information that has international ramifications. International considerations affect STI in at least the following ways:

> *International STI agreements are not uniform in treatment of foreign nations.* The U.S. government's bilateral relations with Canada and Great Britain, for example, are characterized by a level of harmony and cordiality not found in relations with other countries. Some nations are decidedly "more equal" than others in the eyes of the U.S. Hence, when either sending STI to or receiving STI from a given nation, federal STI agencies are bound up within the larger context of U.S. foreign relations with that nation. To put the matter

another way, the U.S. is deliberately not even handed in its dealings with the international community. Policies such as the injunction to disseminate government information in an equal and equitable manner do not transfer directly into the international arena.

International STI agreements vary according to technological strengths and weaknesses of the parties. Certain countries have technological strengths the U.S. wishes to capitalize on. For example, Germany has world class state-of-the-art STI in metals technology, and it is in U.S. interests to acquire German STI in this field. On the other hand, where the U.S. considers its capabilities technologically superior as in aeronautics, the U.S. may resist sharing its STI in order to retain its superiority.

International STI agreements may not extend beyond the parties directly involved. Many if not most international STI agreements stipulate that the agreements pertain only to the signatory parties. A typical agreement might be between the U.S. Department of Defense and the U.K. Ministry of Defense. The agreement may very well preclude sharing of the information beyond DoD, except on a case by case basis, irrespective of the information's security classification status.[9]

Interagency Information Sharing. A-130 looks at information sharing primarily from the standpoint of paperwork reduction, urging agencies to look to one another before collecting new information from the public. Beyond this, A-130 has virtually nothing to say about information sharing. The situation STI agencies find themselves in is somewhat different. As noted above in Chapter IV, budgetary and other considerations are motivating STI agencies to share their existing information and database collections with one another. Agencies could profit from policy guidance on information sharing issues. As matters stand, interagency sharing agreements are being invented from scratch to fit each case. No one is bringing together the collective experience of agencies to formulate some general guidelines.

4. Bringing in Established Policies. Casting a wider net, it is also possible to search out *existing* federal information policy documents that arguably fall within the realm of STI. These documents would be comparable to Statistical Policy Directives in

---

[9]This discussion is substantially based on a personal communication from Kurt Molholm, October 6, 1994.

the sense that they address a specific issue or set of issues rather than a broad sweep of policy. Indeed, several Statistical Policy Directives could be construed as STI directives and brought over into an STI policy. The following areas come particularly to mind, although a systematic search would doubtless yield others.

OMB Circular No. A-16, Coordination of Survey, Mapping, and Related Spatial Data Activities, revised October 19, 1990. Circular A-16 divides up the responsibilities for geographic data among various agencies and provides for coordination of activities. This is clearly an area of STI. Control over the circular has traditionally been exercised by the budget examiners in OMB's Interior Branch, although the most recent revision was principally handled by a member of the OIRA staff (Jack Arthur, who was then on the OIRA staff). In principle, however, there is no compelling reason why OMB's budget side should retain control over this policy area, unless one argues that the division of responsibilities directly affects budget submissions from the various agencies involved. Even so, the argument is hardly compelling.

Policy on Treatment of Human Subjects in Research. The Department of Health and Human Services has a well developed policy statement as to how human subjects should be treated in federally sponsored biomedical research. Again, this is a specialized area of policy that does not apply to the general run of government information but is clearly germane to STI policy.

Statistical Policy Directive No. 16. Standard Classification of Fields of Science and Engineering. On its face, this directive would appear to belong in an STI policy.

Statistical Policy Directive No. 17. Standard Gas Pressure Base. Again, on its face this directive would appear to belong in an STI policy.

Doubtless these examples can be easily multiplied. The area of nuclear research and development would probably yield a number of government-wide STI policies that should be incorporated.

F. Who Would Issue the Policy?

OMB issued Circular A-130 because the Paperwork Reduction Act gave a general information policy function to the Director of OMB and established the Office of Information and Regulatory Affairs (OIRA) as the locus for carrying out the functions. In effect, Congress has decreed that general information policy will be the

province of OIRA.[10]

The scientific and technical area is different. The policy areas enumerated above -- R&D, technology transfer, etc. -- do not rest on the Paperwork Reduction Act but more on the legal and policy basis for federal science and technology. Here the President has a science advisor and authority rests with the Office of Science and Technology Policy (OSTP) within the Executive Office of the President. Hence, the "natural" candidate for issuing an STI policy would seem to be OSTP and the science advisor.

The practical difficulty to lodging responsibility for STI policy in OSTP is that, over the past 15 years or so, OSTP has not taken the initiative in this area despite much urging from outside. Indeed, at present the IITF working group of STI agencies is being convened by OMB as an A-130 implementation study group. OSTP participates in the working group but has shown no signs of desiring to wrest the leadership away from OMB. At the same time, OMB/OIRA possesses slim expertise in STI and is unlikely to originate an STI policy either.

Several points may be noted here. One is that the issue of who should enunciate STI policy is an open question, one that either OMB or OSTP -- or both -- could lay claim to. Another is that neither OSTP nor OMB seems likely to actually do the work of writing the policy, whether from lack of interest or lack of expertise. The work of writing the policy would doubtless fall on the STI agencies themselves. This suggests, in turn, that if the STI agencies went ahead and developed the policy on their own initiative, perhaps both OSTP and OMB would be willing to endorse the work and issue the product as government-wide STI policy.

G. STI Policy and the National Science and Technology Council

In November 1993, President Clinton issued Executive Order 12881 to establish the National Science and Technology Council (NSTC) Not only did NSTC replace the previous FCCSET structure, but the executive order accorded NSTC cabinet level status on a par with the National Security Council. A principal purpose of NSTC is to

---

[10]Within OIRA in the early 1980s, the immediate stimulus for work on what became Circular A-130 was a GAO report, issued in 1983, that contained a "report card" grading OMB's performance on 39 tasks under the Paperwork Reduction Act. (*Implementing the Paperwork Reduction Act: Some Progress, But Many Problems Remain*, Report No. GAO/GGD-83–35, April 20, 1983) One of the tasks in which OMB was given a failing grade was the preparation of general information policy standards and guidelines. In response to the report as well as criticism from Rep. Jack Brooks (D-TX), OMB agreed to begin developing the policy and this effort eventuated in Circular A-130.

establish national goals for federal science and technology investments. NSTC is to develop R&D budget recommendations for OMB to reflect these goals. NSTC has a new committee structure to assist in carrying out its work, and one of the committees is Information and Communication R&D. Moreover, the administration's R&D priorities, as stated in a memorandum from OMB Director Panetta in May 1994, include harnessing information technology in furtherance of national goals.

These developments portend a new structure and atmosphere in which STI policy may well flourish. If the STI community were to develop a policy statement, chances are better than even that a body such as NSTC might endorse and publish the policy.

CHAPTER VII

CONCLUSION

This study has explored the federal information policy environment in which the Defense Technical Information Center finds itself today. The author has attempted to relate DTIC's operational and policy framework to the current fast moving developments in information policy. Particular attention has been devoted to the Freedom of Information Act and intellectual property. The author has also unfolded some of the arguments that can be made for the development of a government-wide policy for scientific and technical information.

A. SUMMARY OF FORECASTS

1. Privacy and Security. In the next year or so, the U.S. will very likely establish some form of Privacy Commission or privacy advisor to the president. One reason for doing so will be in order that the U.S. has an improved official presence in international privacy affairs, as for example in representing U.S. interests with the European Union.

Some limitations on access to public records such as motor vehicle records may be enacted into law by the Congress.

If and when health care reform legislation passes the Congress, the law will include a code of fair health information practices to protect personal privacy in the health field.

Privacy and security of information will continue to be one of the hot topics in the development of the national information infrastructure. The end of the debate over the Clipper chip is not in sight and Congress can be expected to become more heavily involved in information security issues.

2. The Freedom of Information Act. The 104th Congress is likely to be the occasion for amending the Freedom of Information Act to include electronic records. The amendments will attempt to beef up speedy agency compliance with the law and impose new public disclosure requirements on the agencies.

Federal agencies will continue to struggle over the question of what is public information and what is not. Public pressure will continue for making more government information public. The advent of the Government Information Locator Service will exacerbate these questions, particularly with regard to public access to

records systems.

3. **The Paperwork Reduction Act.** Although the Senate finally reached consensus over reauthorizing and amending the Paperwork Reduction Act in late 1994, passage of the PRA bill will remain a secondary priority of the Clinton administration. Strong political support for the PRA is not likely to arise in Congress. A law may pass in the 104th Congress, however, because the general consensus surrounding the PRA, while relatively lukewarm, seems to be in place.

4. **OMB Circular No. A-130.** Circular A-130 has now become more of a consensus document among federal agencies and the public. That consensus may be broken when OMB issues its forthcoming revision to A-130's appendix regarding computer security. Developments within the Information Infrastructure Task Force could also lead to further revisions of the circular.

5. **Government Information Locator Service.** The Government Information Locator Service will definitely be established in 1995. How much effect GILS has remains to be seen, because the open question is the extent to which GILS will become a permanent part of agency IRM operations or an ephemeral phenomenon. GILS will focus more attention on public access to government information, particularly as regards records systems.

6. **The Information Infrastructure.** The Information Infrastructure Task Force will continue as a principal locus of action in federal information policy. To the extent that a national consensus arises on the federal role in the information superhighway, the debate will be located in the IITF.

7. **Intellectual Property.** Demand will grow for agencies to devise policies to manage their intellectual property. Commercial developments in this area may provide some leads for federal agencies. Conflict will continue over the movement toward limited copyright for federal software unless Congress resolves the issue with legislation.

8. **STI and Federal Information Policy.** STI is a subset of all government information that has special policy needs and concerns not addressed in general information policy. Using statistical policy as a guide, one can argue that STI agencies require a government-wide policy directive to address many of their urgent issues, notably, technology transfer, international issues, and interagency sharing. Either OMB or OSTP -- or both -- could issue such a policy. The National Science and Technology Council, in the last analysis, may be an opportune structure for addressing STI policy needs.

B. CONCLUDING RECOMMENDATIONS FOR DTIC

In the author's view, DTIC should watch carefully the ripening of the movement toward GILS. GILS represents both an opportunity and a threat for DTIC. The opportunity arises from the possibility that DTIC could play a pivotal role in DoD in satisfying the GILS requirements. The threat is that the information sources to be included in GILS -- publications, information systems, and records systems -- could have the effect of drying up DTIC's sources in DoD sponsoring agencies. DTIC will be best served if it develops a positive strategy for GILS and takes the offensive.

DTIC also needs to devote some effort to devising a strategy for managing intellectual property in the network environment. This report has suggested that a study of commercial management devices may hold clues for how DTIC can proceed on intellectual property questions.

Imminent events in the world of the Freedom of Information Act, especially the advent of electronic FOIA, will increase the public pressure to make more non-public information public. DTIC will be best positioned to respond to this pressure if it has developed its policy positions in advance. Doing so may entail returning to negotiations with other DoD components concerning the department's FOIA groundrules.

Finally, the author concludes that the federal government does need a government-wide policy statement on STI issues. DTIC can play a leadership role here in promoting the arguments -- before CENDI agencies, OSTP and OMB -- for addressing the preparation of such a statement. If DTIC shows the way by framing the issues for the STI community, it may be much easier to generate consensus in favor of the government-wide STI policy.

APPENDIX A

LIST OF PERSONS INTERVIEWED

Kenneth Allen, President, Information Industry Association

David Appler, DoD Scientific and Technical Information Policy, Defense Technical Information Service, Department of Defense

Toni Carbo Bearman, Dean, School of Library and Information Science, University of Pittsburgh

Jerry Berman, Director, Electronic Frontier Foundation

Jane Bortnick-Griffith, Assistant Chief, Science Policy Research Division, Congressional Research Service, Library of Congress

Elizabeth Buffum, Director of the Office of Scientific and Technical Information, Department of Energy

Beth Duston, Consultant, Washington, DC

Robert Gellman, Acting Staff Director, Subcommittee on Government Information, Justice, and Agriculture, U.S. House of Representatives

Stephen Holden, Senior Policy Analyst, Office of Information and Regulatory Affairs, Office of Management and Budget

Beryl Howell, Senior Counsel, Subcommittee on Technology and the Law, Senate Judiciary Committee

Don Johnson, Director, National Technical Information Service, Department of Commerce

Sarah Kadec, Consultant, Washington, DC

Charles McClure, Professor, School of Information Studies, Syracuse University, Syracuse, NY.

Bruce McConnell, Chief, Information Policy Branch, Office of Information and Regulatory Affairs, Office of Management and Budget

Kurt Molholm, Director, Defense Technical Information Service, Department of Defense

Robert Oakley, Director, Law Library, Georgetown University Law Center

David Plocher, Governmental Affairs Committee, U.S. Senate

Frank Reeder, Deputy Associate Director, Office of Management and Budget

Judy Russell, Director, Electronic Information Dissemination, Government Printing Office

Paul Ryan, Deputy Director, Defense Technical Information Service, Department of Defense

Kent Smith, Deputy Director, National Library of Medicine, Department of Health and Human Services

Ed Springer, Senior Policy Analyst, Office of Information and Regulatory Affairs, Office of Management and Budget

Kenneth Thibodeau, Director, Center for Electronic Records, National Archives and Records Administration

Katherine K. Wallman, Chief, Statistical Policy Branch, Office of Information and Regulatory Affairs, Office of Management and Budget

John Weiner, Director, National Energy Information Center, Energy Information Administration, Department of Energy

Peter Weiss, Senior Policy Analyst, Office of Information and Regulatory Affairs, Office of Management and Budget